energies

MDPI

Article

Assessing Insider Attacks and Privacy Leakage in Managed IoT Systems for Residential Prosumers

Giuseppe De Marco [1,*], Vincenzo Loia [2], Hadis Karimipour [3] and Pierluigi Siano [2]

[1] Evolvere SpA, Via Gustavo Fara, 35, 20124 Milan, Italy
[2] Department of Management and Innovation Systems, University of Salerno, 84084 Salerno, Italy; loia@unisa.it (V.L.); psiano@unisa.it (P.S.)
[3] School of Engineering, University of Guelph, 50 Stone Road East Guelph, Guelph, ON N1G 2W1, Canada; hkarimi@uoguelph.ca
* Correspondence: demarco.giu@ieee.org

Abstract: The transition towards the massive penetration of Renewable Energy Resources (RESs) into the electricity system requires the implementation of the Smart Grid (SG) paradigm with innovative control systems and equipment. In this new context, Distributed Energy Resources (DERs), including renewable sources and responsive loads, should be redesigned to enable aggregators to provide ancillary services. In fact, by using the Internet of Things (IoT) systems, aggregators can explore energy usage patterns from residential users, also known as prosumers and predict their services. This is undoubtedly important especially for SGs facing the presence of several RESs, where understanding the optimal match between demand and production is desirable from several points of view. However, revealing energy patterns and information can be of concern for privacy if the entire system is not properly designed. In this article, by assuming that the security of low-level communication protocols is guaranteed, we focus our attention at higher levels, in particular at the application level of managed IoT systems used by aggregators. In this regard, we provide an overview of the best practices and outline possible privacy leakages risks along with a list of correlated attacks.

Keywords: insider attacks; privacy leakage; IoT systems; aggregators; prosumers

Citation: Marco, G.D.; Loia, V.; Karimipour, H.; Siano, P. Assessing Insider Attacks and Privacy Leakage in Managed IoT Systems for Residential Prosumers. *Energies* **2021**, *14*, 2385. https://doi.org/10.3390/en14092385

Academic Editor: Hugo Morais

Received: 26 February 2021
Accepted: 19 April 2021
Published: 22 April 2021

1. Introduction

The electricity system is facing a growing presence of non-programmable Renewable Energy Resources (RESs). The implementation of modern control systems and equipment and the adoption of novel structures of the distribution electrical system are required. By using new frameworks for the management of scenarios within the energy markets, new flexible Distributed Energy Resources (DERs), considered so far inadequate for ancillary services provisioning, can be considered for the power system needs, including non-programmable renewable sources and demand. A Smart Grid (SG) integrates the actions of all concerned actors to deliver electrical energy in an efficient, secure and economic way. To achieve this goal, the Smart Grid envisions the deployment of Information and Communication Technology (ICT), sensors and smart meters. Moreover, storage systems are allowed at any point of the network, especially at the consumer level. In this way, the SG offers to consumer on the grid the opportunity to become an energy supplier and to be part of the energy trading mechanism. This is the significant for consumers to be transformed into "active energy citizens".

The widespread participation of consumers and prosumers in localized smart electricity markets can be achieved by guaranteeing a reasonable remuneration to all the players for their involvement. However, due to the intrinsic nature of the demand side, finding adequate solutions to allow smooth participation within such markets is still complex. On the

other hand, the regulatory frameworks have not yet made that participation as easy as expected for most consumers [1].

Thanks to the development of electronic technologies spanning from programmable microcontrollers to telecommunication and cloud systems, the design and development of decentralized, secure and transparent architectures are possible. These architectures are aimed at coordinating decentralized optimization schemes and the energy exchanges among prosumers, avoiding investing in centralized control infrastructures. In these architectures, employing a new Energy Management System (EMS) is vital since conventional methods cannot address the additional challenges that originate from the new topology of the network, the utilization of smart devices, and the nature of RESs [2].

The modelling of the aggregator as a Virtual Power Plant (VPP) entity may represent a key for the involvement of consumers [3–5]. Indeed, small and medium-size prosumers can participate in local electricity markets managed by an aggregator, organized as a VPP [6]. In this way, a commercial aggregator organized as a VPP-based business model can exploit the potential flexibility from its prosumers to improve profits stemming from trading within a Local Energy Market (LEM). At the same time, the aggregator can maximize the profits of its consumers and prosumers, who are compensated for their participation.

Commercial aggregators have been entering several European electricity markets (Germany and the Scandinavian region), the USA and Australia.

Many countries are stimulating the experimentation of pilot implementations of VPPs, for instance, Australia, Germany and some of the Nordic countries. U.S. utility companies are also branching out from conventional methods of power generation towards VPPs. In general, the VPP platform links the purchasing, trading and management of decentralized generation assets together with the management of customer demand. Such a platform may enable both distributed generators/prosumers to optimize their assets and it can facilitate customers to lower their energy bills.

IoT employing Advanced Metering Infrastructures (AMIs) plays a key role in the EMS, providing real-time monitoring that allows customers and utilities to supervise consumption patterns and costs [7]. Utilizing a broad range of AMIs, smart devices, gateways, and bidirectional communication systems makes IoT-based platforms more vulnerable in security and privacy [8,9]. At the application level, attacks consist of collecting consumption data at the different levels of the grid and make attackers able to predict customers' daily activities or estimate the number of residents in the house at different times of the day.

The upcoming widespread use of AMIs, along with other smart tools and communication devices, calls for protecting IoE-based smart grids from security and privacy breaches.

These networks are also particularly vulnerable to insider attacks. Service accessibility for an authorized user typically aims to make an illegal profit. It is worth analyzing how such classic attacks can happen in the context of a SG, as a large penetration of RESs is expected by 2050 [10].

There are two types of bidirectional flow of information in a VPP, including User-to-User (U2U) and User-to-Service provider (U2SP). The main emphasis of U2U information exchange is P2P trading, while U2SP aims at energy management and economic issues at the same time. Indeed, aggregation of all participants faces security challenges due to enabling the bidirectional flow of information. Security and privacy have not been investigated well for the VPP paradigm.

This study claims there is a research gap in the application of VPP for energy management, including security and privacy, optimal scheduling, and P2P trading. Additionally, a reliable platform is required to assure P2P trading considering security and privacy since the security challenges are not limited to the physical and economic aspect, and the cybersecurity challenge is indeed vital. However, in this paper, we disregard P2P trading and optimal scheduling of energy resources and we focus on the privacy and security attacks that could be made within such infrastructures.

2. Related Works

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) stated that more than half of the most important attacks reported across all sectors have been conducted on the electrical power system [11]. Employing a massive number of smart devices along with the new generation of communication infrastructures in IoT-based networks opens the gate for cyber and physical malicious behaviors.

Many researchers studied security and privacy concerns in smart grids from different points of view.

Customer privacy has been focused in [12] by defining a categorization of various schemes for AMIs data protection. This work warned that data privacy can be easily endangered by an insider attacker who can also access billing information. A secure certificateless Device-to-Device (D2D) communication authentication mechanism is proposed in [13] to address security issues and privacy risks in D2D communication networks. Han et al. [14] and Ferrag et al. [15] have defined three main contributions in their study including privacy policies, privacy-aware smart metering, and AMI authentication. However, their main focus is on the preservation of privacy. Additionally, preserving the privacy of the data that is collected by AMIs has been investigated in [16]. The practical and technological shortcomings of current privacy protection solutions have been analyzed in [17] focusing on privacy-preserving.

Various aspects of different privacy methods for the smart, such grid as a cyber-physical system, have been reviewed in [18–20]. However, the lack of discussion on the authenticating procedure and smart grid application domain is evident. In [21,22] a comprehensive taxonomy on cybersecurity risks and of AMIs and privacy-preserving smart metering have been presented, respectively.

The Privacy-preserving Aggregation Scheme (PAS) was presented in [23] as a multidimensional arrangement that has a better performance in comparison to the previous methods. The only major disadvantage of the introduced platform is linked to the computational burden that has been assigned to the AMIs. A highly secured trading procedure for incentive-based EMS has been proposed in [24]. The suggested scheme contains different levels including enrollment, key creation, setup, authentication, winner declaration, and incentive claim.

A facilitated methodology employing Password Authenticated Key Exchange (PAKE) was suggested in [25] based on Elliptic Curve Cryptography (ECC). Two main objectives of this work have been focused on authentication and key generation. Elgamal cryptography is another method that has been employed by Vahedi et al. [26] concentrating on data aggregation to preserve AMIs' privacy.

That said, the collection of physical data and the possibility to control the end-users gateway (the EMS) open the door to possible high-level attacks to the user privacy. In this short review, we discuss some lessons learned from a deployed IoT managed system tailored for smart home applications in the context of electricity distribution, by identifying possible privacy leakages and current solutions. Since we will assume a PAN of devices securely configured with the strongest level of low-level security, we do not touch on the problem of privacy or security leakage caused by attack vectors on the low-level protocols. In the following, some findings achieved by deploying a real system used to coordinate energy distribution and control energy storage among members of a community are described. Members could be customers of an Aggregator acting as VPP. Members are supposed to own a smart home gateway which interacts with smart sensors/actuators and a smart meter as well.

An overview of the concepts of IoT system is in Section 3, while the ratio of the system is described in Sections 4 and 5. A brief taxonomy of attacks at the application level is given in Sections 6 and 7.

Finally, in Section 8 we suggest some simple solutions and discuss future works.

3. Cloud-Based IoT Systems

IoT evolved from a pure visionary engineering idea to a massive and successful industrial application of the remote control and measurement of physical appliances [27]. The ubiquity of Internet Protocol (IP) combined with the Artificial Intelligence (AI) and IoT permit a rich set of services supported by smart devices that span from smart homing to remote sensing and industrial machinery control. The concept of Smart Cities heavily relies on IoT. Basically, from the edge side of the communication, IoT systems are composed of a gateway (GW) that controls sensors and actuators within a sort of Personal Area Network (PAN) built on top of some access technologies, like Z-Wave or WiFi. In this context, the system can be managed or unsupervised. Unsupervised IoT systems do not require any intervention from a third party to operate properly. After the installation of the gateway and sensors, no cloud service is invoked. Access to the sensors from outside can be executed in different ways: (1) by using port forwarding; (2) by exploiting the Domain Name System (DNS) [28]; (3) by using public Message Queue Telemetry Transport (MQTT) brokers, etc. The owner of the GW is responsible for the overall management and evolution of her/his system. On the other hand, managed or supervised systems are concerned with controlling and assisting every aspect of the PAN on the edge side. Industrial IoT (IIoT) and service utility providers usually implement this kind of system [29]. Furthermore, managed IoT systems offer a great opportunity for both end-user and service providers in terms of ancillary services. For example, by leveraging cheap virtual data centers and by gaining access to usage patterns of electrical energy, they can furnish an easy tool for the detection of anomalies in electric production or for the recommendation of the wise utilization of appliances' loads. A by-product of similar recommendations is a kind of induced Demand Response policy. In this regard, we claim that managed services are a viable way to realize smart grids at the users' level and offer them additional services for a better approach to the use of electricity, which is more than ever an important environmental problem [30].

Aside from their numerous advantages, smart IoT devices could act as malicious "insiders" capable of spying on their surrounding environment providing valuable intelligence for the attackers [31]. The collection of physical data and the possibility of controlling the end-users gateway opens the doors to possible attacks on user privacy, which still lacks an accepted and unified policy framework [32,33]. Besides that, it also increases the possibility of threats to the real-space, unlike cyber-attacks (DDoS, APT attacks, etc.), which cause damages to cyber-space. If these devices do not ensure strong security, personal information could be easily leaked [34]. We briefly discuss some possible privacy leakages identified in a real deployed IoT managed system tailored for smart home applications in the context of electricity distribution. Although we will assume a PAN of Z-Wave devices securely configured with the strongest level of low-level security, we do not touch the privacy leakage caused by attack vectors on the low-level protocol. The system is supposed to be owned by an aggregator acting as a VPP, where all aggregator's members are equipped with a smart home gateway that interacts with smart sensors/actuators and smart meters.

3.1. Deployed Architecture

A complex IoT system aimed at providing end-users with both smart homing applications and value-added services for better electricity usage has been implemented for evaluation at the aggregator level. The schematic representation of the system is given in Figure 1. The architecture is logically divided into two distinct planes: (1) The Power Plane (PP) and (2) Market Plane (MP). In the MP, we find the IoT remote manager (see Section 5), which contains all the software services to run the aggregator functions, e.g., the Oracles for forecasting of energy usage and the drivers for sending command towards the smart meters (DR and CM). The MP can also implement optimization functions to trade energy quantities in the energy market. In the PP, we have the interface towards the electricity grid, i.e., the distribution network. Smart meters, for example, are directly connected to the distribution grid. The information bridge between the PP and the MP is the Home Gateway (HGW), which interacts with the sensors (M) and actuators (A) connected to

the PP. As said, these devices can be smart home devices or smart meters connected to production systems from RES such as photovoltaic plants. The HGW communicates with the central cloud to store measurement data and receive commands for configuration and tele assistance. In the case of energy aggregators, the IoT Remote Manager (IRM) can also be used to monitor the overall energy availability and to formulate economic offers on the energy markets.

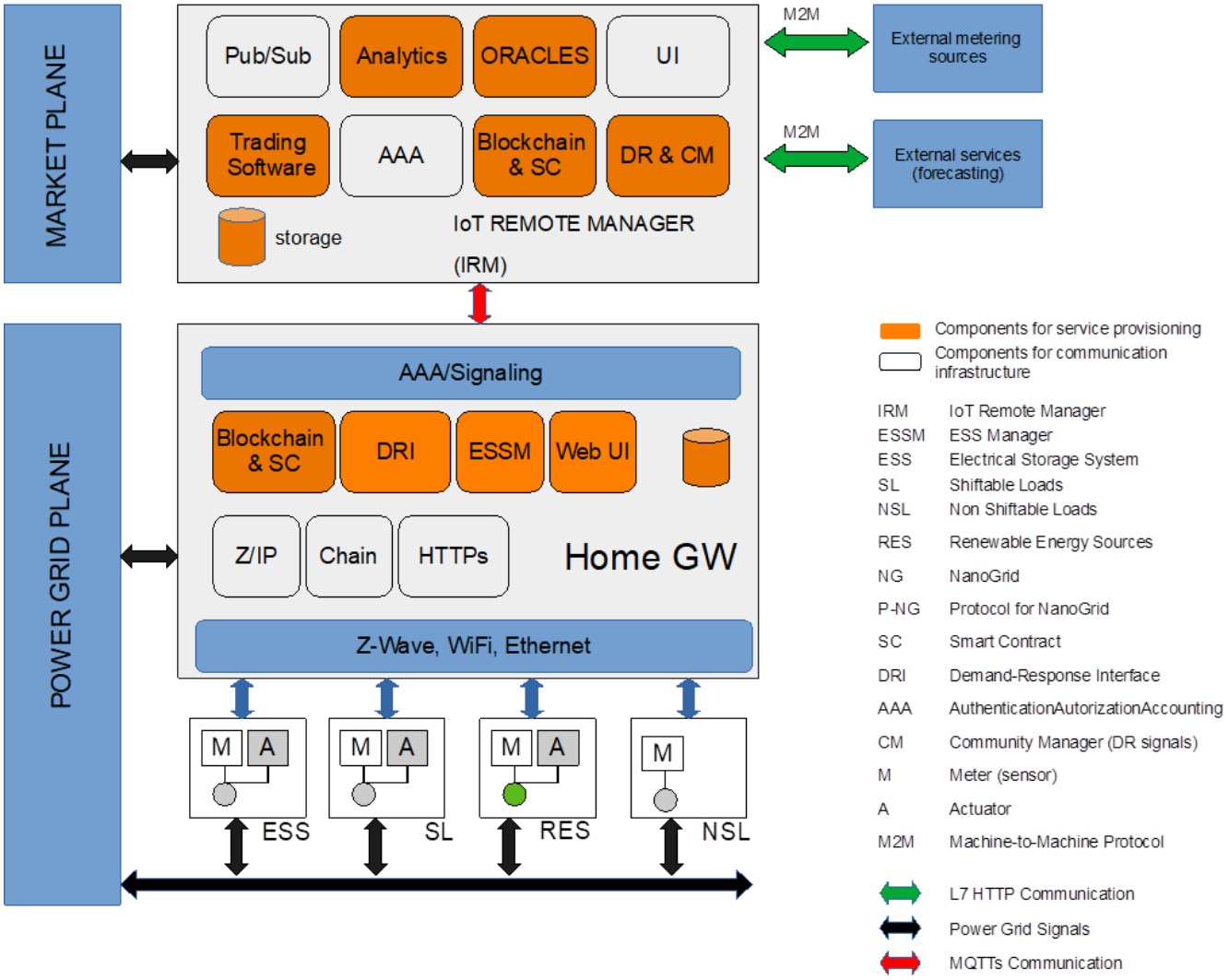

Figure 1. Schematic representation of the deployed IoT system. Z/IP refers to the Zwave interface software, and Chain is a powerline data protocol to acquire information from the smart meter.

From the aggregator point of view, the most important component in the PAN is the smart meter, which is a device capable of measuring and transmitting energy consumption and production data. The meter is smart because it can be remotely controlled using custom functions that are accessed by dedicated commands issued on MQTT channels.

An open IoT architecture has been employed to cope with many prosumers with different electrical appliances and a centralized database has been implemented to record their energy data.

3.2. Communication Protocols

From the point of view of communications among all components of the system, the system is based on guidelines presented in [30] and it can be depicted in Figure 2.

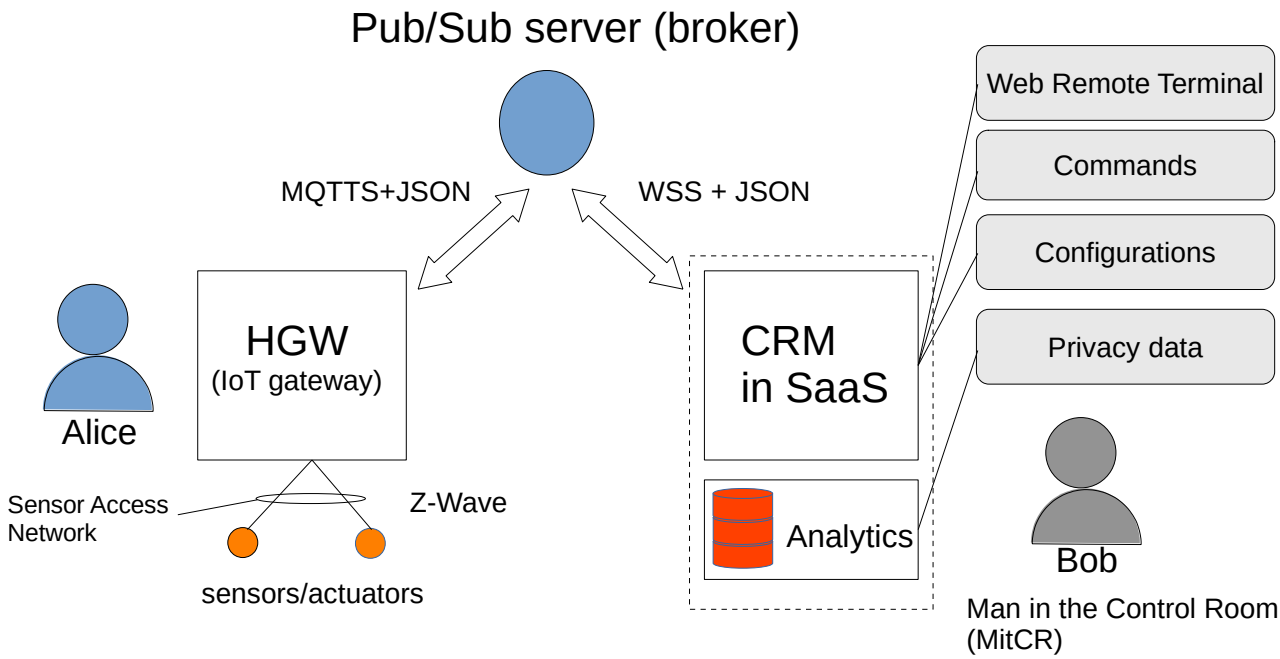

Figure 2. The core components of a managed Internet of Things (IoT) system is the Publisher/Subscriber (Pub/Sub) broker which broadcasts messages from subscribed members. Customer Relation Management (CRM); Home Gateway (HGW); Software as Service (SaaS).

Usually, such systems use the Publisher/Subscriber (Pub/Sub) communication pattern, where a central communication component called broker acts as a broadcasting server. The broker is a fire-and-forget server: it simply dispatches packets to a plethora of subscribed members, which in turn publish messages to authorized channels, also known as rooms or topics. The most used asynchronous protocol for such a communication is the MQTT [35] and its secure version MQTTS, because of its simplicity and flexibility. In this case, a member is an MQTT client running within the HGW. The HGW collects sensor readings and dispatches commands to actuators. The readings are sent on special channels using MQTT. Similarly, commands are issued from the Customer Relation Management (CRM) on separate channels. The operator "Bob" theoretically has access to much of the end-user information, and to some extent, by invoking the classic image of the Man In the Middle (MitM), he can be depicted as the Man in the Control Room (MitCR) in the context of privacy of managed IoT systems.

Encapsulating MQTT in secure WebSockets (wss) is possible and, in fact, the developed web-based management software or CRM in Software as Service (SaaS) uses wss to interact with the remote HGW. Every single application message exchanged between the HGW, the CRM and the broker is formatted along with the JSON standard. This permits the description of the services and operations in terms of textual schemata [36]. The application messages can be related to the configuration of the end-user device, special command for the PAN or for the Operating System (OS) itself.

4. The Home GW (HGW)

The implemented GW is composed of: (1) a Raspberrylike System on Board, a board based on the Broadcom microprocessor; (2) an interface shield containing various additional microchips, such as Z-Wave, WiFi and others for dedicated functions. The OS is based on Linux Debian. The HGW has been developed in nodejs, a very popular JavaScript engine based on the V8 JavaScript interpreter by Google, because of its simplicity to build real-time asynchronous communications. The components of the HGW are shown in Figure 1.

Besides conventional components used for communications and configuration like Web servers for User Interface (UI), Authentication Authorization and Accounting (AAA)

for basic application security, other components related to P2P trading have been implemented (not discussed here) for future evaluation. Most sensors and actuators are used to collect energy data; others are smart home gadgets, such as smart lamps, motion sensors, fire alarms, etc. Indeed, some of these smart home devices can also measure local energy consumption, which is the most valuable piece of data for the aggregator. For example, smart wall plugs can easily report these values. The HGW is plugin-oriented, e.g., every new technology can be installed by developing a particular software module that interacts with the core module through a custom protocol. An important plugin of the HGW is the Energy Storage System Manager (ESSM), which controls the Energy Storage Systems (ESSs) from different vendors. We used a rack of commercial lithium batteries in our settings, which can be controlled by employing JSON Rest API. The ESS can work autonomously by using internal algorithms which guarantee the maximization of self-consumption of the energy. When tied with Renewable Energy Sources (RES) systems, the ESS is charged when a photovoltaic energy production excess occurs.

As for the completeness of the presentation, we cite the fact that the ESSM can bypass the ESS algorithms to share accumulated energies among other users or, in the case where the IRM is also used by an aggregator, to sell excess or unused energy to the energy market. These decisions are enabled by explicit approval from end-users. Indeed, the direct control of the ESS can be a source of attack vectors.

5. IoT Remote Manager

The core component of our managed system is the MQTTs broker, which has been implemented from scratch. It supports AAA, i.e., every HGW is associated with a particular room and with basic Quality of Service (QoS). We use QoS 0 (no reliability of messages) for MQTT and QoS 1 (basic reliability) for remote commands. The broker is responsible for coordinating commands and collecting sensing data. It permits ubiquitous communications without any intervention on the end-user network components. Moreover, other components, such as ORACLES for energy forecasting, Analytics for obtaining insights from aggregate energy usage, and Smart Contracts for future applications of transactive energy, have been implemented to realize added services.

5.1. Demand Response and Smart Grids

In the proposed system, the HGW can also interact with shiftable loads, i.e., electrical usage patterns can be shifted in time. This is the basis of Demand Response (DR), a wider topic concerning a better utilization of the distribution grid, especially for congestion risk avoidance and energy resource planning [37]. Although realizing direct DR at a residential level is not still considered an immediate target, the implemented system can collect energy data and suggest to the user with some hints to lower consumption and obtain incentives.

This kind of soft or induced DR turns out to be undoubtedly useful when the community of managed users is also equipped with RES and ESS. In this case, the user is called a prosumer, and she/he will be incentivized to use energy when the predicted RES production is high.

5.2. Tools and Functions

In a managed IoT system, remote access to the HGW to solve misconfigurations or to debug anomalies reported by the end-user is essential. One possible solution is to deploy one or more VPNs among all the connected clients to accomplish this need. This solution has turned out to not be so easily scalable with the number of gateways, and it is, actually, redundant because we already have a central dispatcher component: the MQTT broker. Consequently, we recast the problem by engineering a remote web shell, i.e., a terminal which can be run inside a web browser.

As shown in Figure 3, the web shell sends messages to the broker, which in turn broadcasts them toward a special room of the MQTT communication. On the HGW side, an MQTT client redirects shell messages toward a terminal or shell emulator, e.g., xterm.

In this way, a web shell can be opened directly on the user's HGW. The AAA mechanisms guarantee security; to access the web terminal, the operator must be authenticated and authorized.

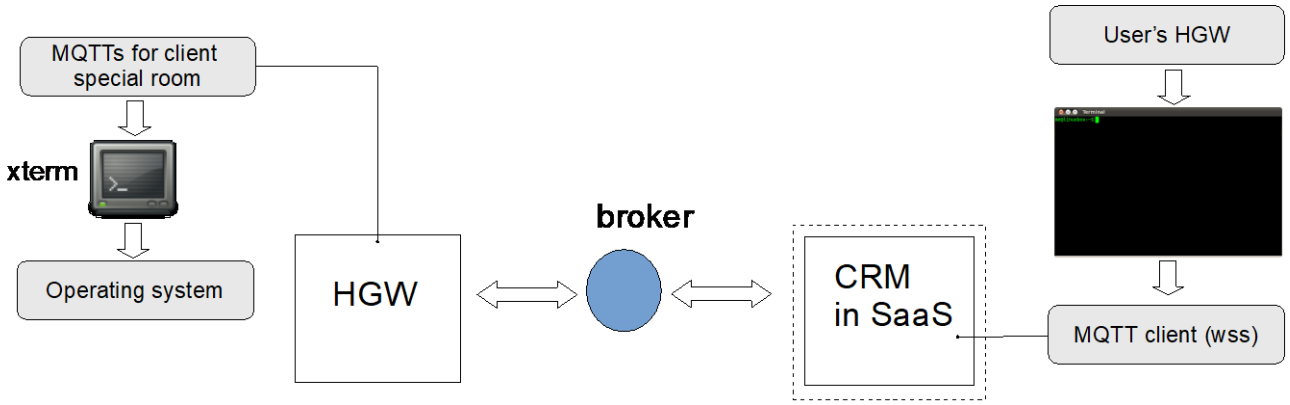

Figure 3. Remote Web Terminal used for support operations.

Theoretically, an authenticated operator can also send commands to actuators or, badly, to the ESS system. The authorization to such an action is sometimes unavoidable because the service-oriented nature of the aggregator concerns the full support of the end-user. Therefore, any technical problem should be debugged and solved remotely. This model is similar to that used by some telecommunications companies, which provide the end-user with a rented ADSL modem by inherently assuming that the remote control is taken for granted. These tools and functions proved to be beneficial for the deployment of the services, but from the privacy point of view, they put many responsibilities in the hands of the operators. We try to synthesize them in the following sections.

6. Privacy Leakage

In general, the security of networked sensors (for home applications) can be analyzed by using a combination of attack models and privacy leakage risk models. Attack models concern the classification of dangerous behaviors at different layers of the information and communication stack. Such attacks can be performed by exploiting software bugs or misconfigurations of protocols and devices. For example, in ad hoc Z-Wave networks, if non-secure Z-Wave nodes are present, stealing the control and performing a reply attack is relatively simple [38,39]. Usually, this kind of communication security is solved by adopting advanced and updated protocols. For instance, in the case of Z-Wave, to lower the probability of such an event, in 2016, the Z-Wave Alliance has issued the mandatory implementation of the S2 protocol, which is based on ECDH secure keys exchange [40]. However, there are also high-level attacks, i.e., attacks that exploit misconfigurations and, theoretically, could be executed from within the IRM. Finally, side attacks are attacks that are built on the disclosure of patterns. Although the likelihood of such attacks is low, they can cause damages or compromise privacy. In this context, attacks and privacy leakage are synonyms, i.e., they point out attacks that can compromise privacy. In other words, attacks on low-level protocols are relatively hard to accomplish for well-designed networks, and we take protocols security for granted.

To some extent, the greater the centralization of control actions, the higher the number of privacy leakages that can happen. We counted possible privacy leakages in Table 1.

Table 1. Possible privacy leakage carried by an insider attack.

	Information	Potential Leakage
1	Energy patterns	Behavior, User presence, User activity,
2	Sensor Data (Motion)	User presence, User habits, User activity
3	Sensor Data (Actuators, Plugs, Lamps)	Impersonation, Trading interference

Since information is centralized, the type of leakage is connected with patterns found in the collected information. These patterns, at least theoretically, could reveal:

- User activity: by correlating many patterns related to energy consumption, one could track the habits of users and intentionally provoke outages or promote outside marketing operations (outsider–insider marketing).
- User presence: by correlating patterns related to motion sensors, one could reason about the probability that the user is in the house or when she/he leaves it. The same could be done by correlating energy consumption usage.

For example, the energy consumption patterns of a typical residential user are shown in Figure 4. The measures traced reveal a daily pattern between 09:00 and 15:00. The power increase around noon could indicate the presence of inhabitants, maybe because the household is composed of children coming back from school who switch on their computers, TVs or air conditioning systems.

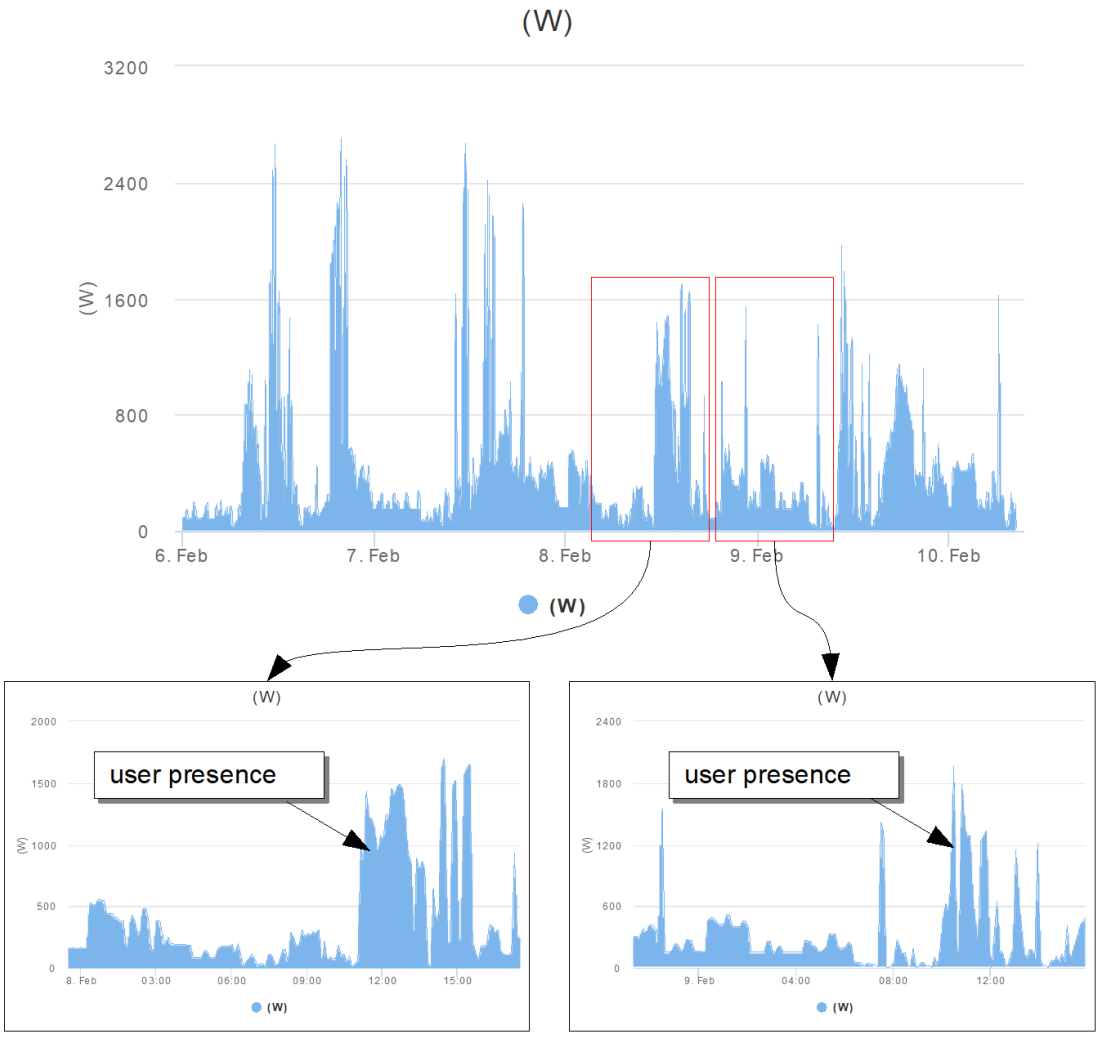

Figure 4. Power usage for a typical residential context. The traces have been recorded during the year 2021. All these possibilities are at the desk of the operator if no other countermeasures are taken. We will give some solutions in the upcoming sections.

Other actions regard the misuse of commands: one can impersonate an alarm by sending, for example, commands to activate a smoke or waterflood alarm.

7. Attack Models

By exploiting remote HGM, one could, at least theoretically, perform the attacks listed in Table 2. We assign a subjective level of difficulty on a scale of three possible values: low, medium, high. Every attack vector refers to necessary tools to be performed. For each attack vector, the correspondent security principle is shown.

For example, for the first attack in Table 2, by using the Secure Shell (SSH), which is a tool normally installed in the embedded OSs, one could easily install an audio forwarding script by realizing an audio spy bug. This attack needs a microphone on the HGW. However, with some work, it could be possible to use the HGW as a trojan horse to discover microphone-equipped devices within the local network of the HGW. SSH can also be used to install an anonymous proxy or to tunnel and hide external communications. In this case, privacy is compromised because, if the tunnel is used for malicious actions, the user information (IP and location) is disclosed. In the case of severe consequences of this kind of attack, the HGM could be reset to factory defaults by reducing the service level perceived by the end-user.

Redhat Package Manager (RPM) is used to pack software and related scripts to install the core system's updates. A well-forged packed RPM could contain malware or trojan horses.

Such attacks are very difficult to implement. For example, RPM cannot install software on locations protected by strict Authorization Control List (ACL) rules. Audio spy is difficult without an on-board microphone. Sniffing or eavesdropping on user's Local Area Network (LAN) traffic is nearly impossible if no packet analysis tools, such as tcpdump, are installed in the operating system. Additionally, Address Resolution Protocol (ARP) poisoning is impossible if no arp binaries are installed. However, by using SSH one could download customized binary versions of this tool and start related misuses. Maybe the simplest attack is jamming: by flooding the user's LAN with a high ping packets rate, one could at least disrupt the usual utilization of network traffic. This could be a problem if the user's LAN contains critical devices, such as medical ones. However, saturating a gigabit's LAN is relatively hard [41].

It should be clear that these attack models are insider attacks, i.e., they can be initiated not by a MitM but by a MitCR. For this reason, some kind of traceability and anonymity are necessary.

Table 2. Potential misuses of software tools installed into the Internet of Things (IoT) Home Gateway (HGW).

	Tool/Software	Example	Difficulty	Targeted Security Principle			
				Confidentiality	Integrity	Accountability	Availability
1	ssh	Audio spy Hidden proxy Hidden tunneling	High/Medium	x			
2	rpm	Install unwanted software	High	x			
3	ping	Jamming	Easy				x
4	bash	Shut down Erasing everything	Low		x		x
5	arp	MitM MitCR		x	x	x	x
6	tcpdump	Eavesdropping of LAN traffic	Low	x			
7	wget, scp	Download custom binaries	High				

8. Solution and Proposals

Our considerations are pragmatic and based on the maturity of our experience. Some attack vectors are really difficult to implement or rather impossible. However, to protect user privacy, we propose the following actions, which are easy to implement.

Traceability: Every action in the IRM should be traceable and persistent. The higher privilege the operator has, the higher the verbosity level that should be applied in order to trace the performed actions. First-level operators usually do not perform complex operations and do not use debugging tools and traceability. However, second-level operators could use debugging tools as the web terminal previously described. A possible solution could be the tracing of every single command or message issued in the terminal. As shown in Figure 5, an additional component, namely the tracer, could listen on special topics of the MQTT broker, e.g., #operations/*, and store the relative messages on a dedicated log database, easy to query. For example, one could use an unstructured database or NoSql database such as MongoDB [42] which natively supports JSON data. Then, a Machine Learning (ML) algorithm trained for detecting malicious patterns can be used to infer the class of the logs, for every session of the web terminal. Alerts are sent to the services responsible for access management and monitoring.

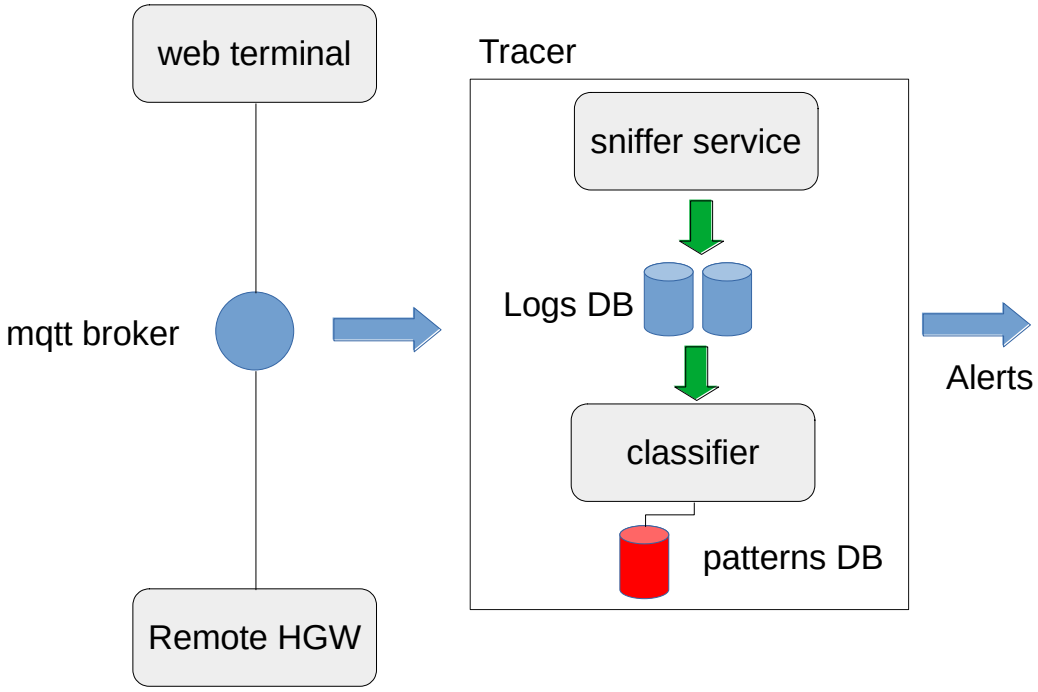

Figure 5. Schematic representation of a tracer for detecting misuses of the web terminal. The malicious patterns are stored in a Database (DB).

Anonymity: Revealing user details of information patterns such as energy usage should be impossible for operators at all layers. The user shall be identified by an anonymous HGW, as happens in permissioned blockchains used for economic transactions where the user identity associated with the digital wallets is never revealed. However, leveraging the full anonymity of blockchain in this context and its pros and cons is a matter of current evaluation.

Aggregating: By applying some non-invertible function to information patterns, the leakage is reduced if not removed entirely. For example, one could show only aggregates, i.e., sums of energy consumption and production.

Locality: For some services based on energy predictions, individual energy patterns, and not aggregates, are needed. To solve the reveal-or-not reveal dilemma, automatic and anonymous suggestions should be executed locally, e.g., by using local ML inference.

For instance, one could anonymously train ML regression models in the cloud and then run the inference on the edge, i.e., in the HGW. In this way, the suggestion for better energy usage, or the soft DR, can be built by training neural networks in the IRM. Once the model has been trained, it is downloaded into the HGW where the inference happens. In this way, no pattern is disclosed in the IRM and actions are computed only at the edge, i.e., where the user owns everything.

9. Conclusions

In this paper, we elaborate on our experience stemming from building an experimental cloud-based IoT system conceived for applications and services in the domain of residential energy distribution. Usually, similar systems are used by energy aggregators acting as VPPs. Accordingly, we named these systems "managed IoT systems". The benefits of centralized control of smart home GWs are real for both the aggregators and the end-user who could be gradually guided towards a better usage of the energy resources. However, centralizing is always a warning flag for privacy leakages. We discussed some of the more common attacks on privacy. Although some of them are very difficult to perform, they should be taken into account when designing a robust control room to prevent any fraudulent utilization of tools and functions. To increase security and privacy in this context, the evaluation of real test-beds based on the blockchain world is ongoing.

Author Contributions: Supervision, H.K. and P.S.; Validation, V.L.; Writing—original draft, G.D.M.; Writing—review & editing, G.D.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The present work has been developed within the supervision of Domenico Cimmino who carefully followed all the management complexities that arose during the project.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sharifi, R.; Fathi, S.; Vahidinasab, V. A review on Demand-side tools in electricity market. *Renew. Sustain. Energy Rev.* **2017**, *72*, 565–572. [CrossRef]
2. Lee, C.-H.; Lai, Y.H. Design and Implementation of a Universal Smart Energy Management Gateway based on the Internet of Things Platform. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–11 January 2016; pp. 67–68.
3. Faria, P.; Spínola, J.; Vale, Z. Reschedule of Distributed Energy Resources by an Aggregator for Market Participation. *Energies* **2018**, *11*, 713. [CrossRef]
4. Shen, B.; Ghatikar, G.; Lei, Z.; Li, J.; Wikler, G.; Martin, P. The role of regulatory reforms, market changes, and technology development to make demand response a viable resource in meeting energy challenges. *Appl. Energy* **2014**, *130*, 814–823. [CrossRef]
5. Carreiro, A.M.; Jorge, H.M.; Antunes, C.H. Energy management systems aggregators: A literature survey. *Renew. Sustain. Energy Rev.* **2017**, *73*, 1160–1172. [CrossRef]
6. Peter Asmus, How Real are Virtual Power Plants?, Powergrid International, Volume 19, Issue 11, Dallas, TX, USA. Available online: https://www.power-grid.com/der-grid-edge/how-real-are-virtual-power-plants/ (accessed on 22 April 2021).
7. Said, O.; Al-Makhadmeh, Z.; Tolba, A. EMS: An Energy Management Scheme for Green IoT Environments. *IEEE Access* **2020**, *8*, 44983–44998. [CrossRef]
8. EG3 Report–Smart Grid Task Force, Regulatory Recommendations for the Deployment of Flexibility. January 2015. Available online: https://www.jstor.org/stable/26377527?seq=1 (accessed on 22 April 2021).
9. Rouzbahani, H.M.; Karimipour, A.R.H.; Dehghantanha, G.S.A. *Anomaly Detection in Cyber-Physical Systems Using Machine Learning, in Handbook of Big Data Privacy*; Springer: Cham, Switzerland, 2019; pp. 219–235.
10. Li, H.X.; Edwards, D.J.; Hosseini, M.R.; Costin, G.P. A review on renewable energy transition in Australia: An updated depiction. *J. Clean. Prod.* **2020**, *242*, 118475. [CrossRef]

11. Rouzbahani, H.M.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. Blockchain Applications in Power Systems: A Bibliometric Analysis. December 2019. Available online: http://arxiv.org/abs/1912.02611 (accessed on 21 January 2020).
12. Zhong, C.L.; Zhu, Z.; Huang, R.G. Study on the IoT architecture and gateway technology. In Proceedings of the 14th International Symposium on Distributed Computing and Applications for Business, Engineering and Science, DCABES 2015, Guiyang, China, 18–24 August 2016.
13. Tan, H.; Song, Y.; Xuan, S.; Pan, S.; Chung, I. Secure D2D Group Authentication Employing Smartphone Sensor Behavior Analysis. *Symmetry* **2019**, *11*, 969. [CrossRef]
14. Han, W.; Xiao, Y. Privacy preservation for V2G networks in smart grid: A survey. *Comput. Commun.* **2016**, *91–92*, 17–28. [CrossRef]
15. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustain. Cities Soc.* **2018**, *38*, 806–835. [CrossRef]
16. Asghar, M.R.; Dan, G.; Miorandi, D.; Chlamtac, I. Smart Meter Data Privacy: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2820–2835. [CrossRef]
17. Desai, S.; Alhadad, R.; Chilamkurti, N.; Mahmood, A. A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure. *Clust. Comput.* **2018**, *22*, 43–69. [CrossRef]
18. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential Privacy Techniques for Cyber Physical Systems: A Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 746–789. [CrossRef]
19. Wang, T.; Zhang, X.; Feng, J.; Yang, X. A Comprehensive Survey on Local Differential Privacy toward Data Statistics and Analysis. *Sensors* **2020**, *20*, 7030. [CrossRef] [PubMed]
20. Said, O.; Albagory, Y.; Nofal, M.; Al Raddady, F. IoT-RTP and IoT-RTCP: Adaptive Protocols for Multimedia Transmission over Internet of Things Environments. *IEEE Access* **2017**, *5*, 16757–16773. [CrossRef]
21. 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]
22. Sultan, S. Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey. *Comput. Secur.* **2019**, *84*, 148–165. [CrossRef]
23. Zhang, L.; Zhang, J.; Zhang, J. EPPRD: An Efficient Privacy-Preserving Power Requirement and Distribution Aggregation Scheme for a Smart Grid. *Sensors* **2017**, *17*, 1814. [CrossRef] [PubMed]
24. Rahman, M.S.; Basu, A.; Kiyomoto, S.; Bhuiyan, M.Z.A. Privacy-friendly secure bidding for smart grid demand-response. *Inf. Sci.* **2017**, *379*, 229–240. [CrossRef]
25. Vahedi, E.; Bayat, M.; Pakravan, M.R.; Aref, M.R. A secure ECC-based privacy preserving data aggregation scheme for smart grids. *Comput. Netw.* **2017**, *129*, 28–36. [CrossRef]
26. Sun, Z.; Song, C. Security and Privacy-Preserving Metering Service in the Smart Grid. *Int. J. Commun. Netw. Syst. Sci.* **2017**, *10*, 307–315. [CrossRef]
27. Arasteh, H.; Hosseinnezhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-Khah, M.; Siano, P. Iot-based smart cities: A survey. In Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, 7–10 June 2016; pp. 1–6.
28. Jin, Y.; Tomoishi, M.; Fujikawa, K.; Kafle, V.P. A Lightweight and Secure IoT Remote Monitoring Mechanism Using DNS with Privacy Preservation. In Proceedings of the 2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–2. [CrossRef]
29. Xu, H.; Yu, W.; Griffith, D.; Golmie, N. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. *IEEE Access* **2018**, *6*, 78238–78259. [CrossRef]
30. Siano, P.; De Marco, G.; Rolan, A.; Loia, V. A Survey and Evaluation of the Potentials of Distributed Ledger Technology for Peer-to-Peer Transactive Energy Exchanges in Local Energy Markets. *IEEE Syst. J.* **2019**, *13*, 3454–3466. [CrossRef]
31. Haddad Pajouh, H.; Dehghantanha, A.; Parizi, R.M.; Aledhari, M.; Karimipour, H. A survey on internet of things security: Requirements, challenges, and solutions. *Internet Things* **2019**, 100129, in press. [CrossRef]
32. Thorburn, R.; Margheri, A.; Paci, F. Towards an integrated privacy protection framework for IoT: Contextualising regulatory requirements with industry best practices. In Proceedings of the Living in the Internet of Things (IoT 2019), London, UK, 1–2 May 2019; pp. 1–6. [CrossRef]
33. Khan, M.A.; Noor, F.; Ullah, I.; Rehman, S.U.; Nisar, S.; Ahmad, M. An Efficient Medium Access Control Mechanism for Flying Ad-hoc Networks. *Comput. Syst. Sci. Eng.* **2021**, *38*, 47–63. [CrossRef]
34. Dovom, E.M.; Azmoodeh, A.; Dehghantanha, A.; Newton, D.E.; Parizi, R.M.; Karimipour, H. Fuzzy pattern tree for edge malware detection and categorization in IoT. *J. Syst. Arch.* **2019**, *97*, 1–7. [CrossRef]
35. Message Queuing Telemetry Transport (MQTT), ISO. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/94/69466.html (accessed on 5 August 2020).
36. JSON Schema. Available online: https://json-schema.org/ (accessed on 22 April 2021).
37. Ruzbahani, H.M.; Rahimnejad, A.; Karimipour, H. Smart Households Demand Response Management with Micro Grid. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019. [CrossRef]

38. Rouch, L.; François, J.; Beck, F.; Lahmadi, A. A Universal Controller to Take Over a Z-Wave Network. 2017. Available online: https://www.blackhat.com/docs/eu-17/materials/eu-17-Rouch-A-Universal-Controller-To-Take-Over-A-Z-Wave-Network-wp.pdf (accessed on 22 April 2021).
39. Celebucki, D.; Lin, M.A.; Graham, S. A security evaluation of popular Internet of Things protocols for manufacturers. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018. [CrossRef]
40. Barker, E.; Chen, L.; Roginsky, A.; Vassilev, A.; Davis, R. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
41. Ajayan, A.C.; Prabaharan, P.; Krishnan, M.R.; Pal, S. Hiper-ping: Data plane based high performance packet generation bypassing kernel on ×86 based commodity systems. In Proceedings of the 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 21–24 September 2016; pp. 478–483. [CrossRef]
42. Mongo DB The application data platform. Available online: www.mongodb.com (accessed on 22 April 2021).