IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Received June 29, 2019, accepted July 15, 2019, date of publication August 8, 2019, date of current version August 22, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2933859

Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service

CHANG CHOI[1], (Senior Member, IEEE), AND JUNHO CHOI[2]
[1]IT Research Institute, Chosun University, Gwangju 61452, South Korea
[2]Division of Undeclared Majors, Chosun University, Gwangju 61452, South Korea

Corresponding author: Junho Choi (xdman@chosun.ac.kr)

This work was supported in part by the Korea Electric Power Corporation under Grant R18XA06-12, and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (Ministry of Science and ICT) under Grant 2017R1E1A1A01077913.

ABSTRACT For a variety of cyber-attacks occurring in a power IoT-Cloud environment, conventional security intrusion incident detection and response technologies typically use pattern- and behavior-based statistical methods. However, they cannot provide fundamental solutions for a security intrusion or attacks, which are becoming more intelligent and diverse as time passes. Therefore, an effective response method that can respond to security intrusions intelligently while using an access control technique based on ontology reasoning is required. This can be achieved by adopting a variety of intelligent reasoning technologies for security intrusion incidents of power systems, such as various reasoning technologies based on the ontology and semantic-web technologies being actively studied in the field of intelligent systems, and malicious code detection technologies based on an intelligent access control model, text mining, and natural language processing technologies. Accordingly, a security context ontology was modeled by analyzing the security vulnerabilities of a power system in a power IoT-Cloud environment, and security context inference rules were defined. Furthermore, this paper presents an appropriate power IoT-Cloud security service framework that can be used in a power IoT-Cloud environment. In addition, a security mechanism that can be efficiently operated in such an environment is implemented. In experiments conducted for this application, attack context scenarios that commonly occur were created using a smart meter as an example, which is an essential power system device. Inference rules were then composed for each attack stage to check the paths of attacks those that exploit the vulnerability of a smart meter system. As a result, it was confirmed that a high level attack detection results can be obtained based on the inference rules.

INDEX TERMS Power system security, IoT, ontology modeling, security ontology, context reasoning

I. INTRODUCTION

As Internet of Things (IoT) devices are becoming more diverse and are rapidly increasing in number, the issues of energy-efficient data transmission and collection, and sensor allocation and management, have emerged in environments with large numbers of sensors composing the IoT owing to their low power and limited computational capability. In particular, new security problems have emerged, such as a limitation of storage capacity and security vulnerabilities, in addition to private information protection problems caused by key management issues, and such problems should be promptly solved. Accordingly, attempts have been made to solve these limitations of IoT by utilizing the advantages of cloud computing [1]. Through a new service paradigm, namely, the convergence of IoT and cloud (IoT-Cloud), cloud resources can be shared, based upon which, functions are provided for a virtualization of physical resources, maximization of resource use, and location-independent ubiquitous accessibility. In such a IoT-Cloud environment, services of the cloud computing domain should provide reliable security in terms of data processing and storage, and guarantee information protection with respect to data confidentiality, availability, and integrity. Moreover, security vulnerabilities can occur during the process of operating an IoT-Cloud convergence environment and generating and processing the data. Therefore, reliable and safe accessibility and connectivity are required in terms of safe data transmission and management.

A smart-grid is a typical application of such an IoT-Cloud service. A smart-grid is an intelligent power grid

The associate editor coordinating the review of this manuscript and approving it for publication was J-H Lee.

that optimizes the energy efficiency by allowing power suppliers and consumers to exchange real-time information bi-directionally by combining a conventional unidirectional power grid with information technology [2]. In a smart-grid, a variety of the latest information and communication technologies are used, such as an advanced metering infrastructure (AMI), IoT technology, cloud computing, and smart metering technology. For this reason, new security threats may occur that have not taken place in conventional environments. Because machines and devices are operated in a connected environment, an external connection between systems has become indispensable, and attacks that abuse security vulnerabilities of wireless communication have become possible. As smart grid technologies progress, they are expected to be exposed to a variety of cyber-attacks. Compared to amount damage to other infrastructure, an attack on a power system can induce an enormous amount of damage across the entire nation [4]. For conventional security intrusion incident detection and response technologies of a power system, pattern- and behavior-based statistical methods are typically used, but are not fundamental solutions for security instruction and attacks, which are becoming increasingly more intelligent and diverse. Therefore, an effective response method that can respond to security intrusions intelligently while using an access control technique based on ontology reasoning is required. This can be achieved by adopting a variety of intelligent reasoning technologies for security intrusion incidents of power systems, such as various reasoning technologies based on ontology and semantic-web technology that are being actively studied in intelligent systems, and malicious code detection technologies based on an intelligent access control model, text mining, and natural language processing technologies [4].

Accordingly, in this paper, a security context ontology is modeled by analyzing the security vulnerabilities of a power system in power IoT-Cloud environment, and the security context inference rules are defined. Furthermore, this paper presents an appropriate power IoT-Cloud security service framework that can be used in a power IoT-Cloud environment and implements a security mechanism that can be efficiently operated in that environment.

In Section 2, the current status of power IoT-Cloud security and ontology-based security context reasoning is briefly discussed as a theoretical background. In Section 3, a power IoT-Cloud security service framework designed for ontology-based security context reasoning for the power IoT-cloud security service proposed in this paper is detailed. Moreover, the power IoT-Cloud security contexts are defined and the designed ontology, security context reasoning module, and rules are described. In Section 4, the inference rule design used in the experiments is provided, and based on these experiments, the inference rules are examined. Finally, in Section 5, some concluding remarks along with a description of a future study.

II. RELATED WORKS

A. CURRENT STATUS OF POWER IOT-CLOUD SECURITY

An IoT environment can be classified broadly into three technical domains: first, the device domain for the IoT device sensor, processor, connecting device, and operating system; second, the connectivity domain connecting the IoT devices with wired/wireless Internet networks; and third, the platform domain, which provides technologies for data and information generation and analysis [5]. Because the devices used in an IoT environment have limitations such as low power, low capacity, and limited performance, an efficient service will be created by combining them with cloud computing technology. An IoT-Cloud environment that combines cloud computing and IoT is constructed as shown in Fig. 1.

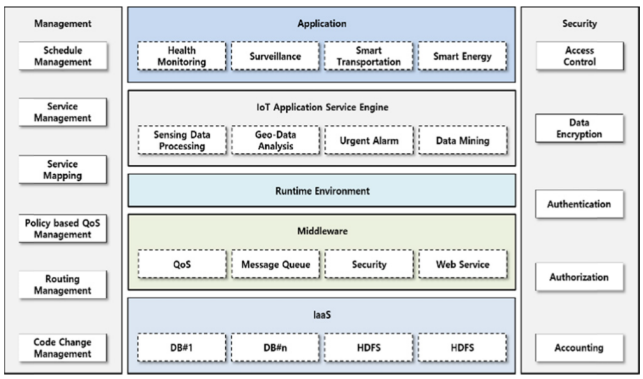

FIGURE 1. IoT-Cloud framework.

An IoT-Cloud environment consists of an embedded system, sensors, multi-service edge, core, data center, and cloud, among other aspects. Such an IoT-Cloud environment can use resources efficiently based on the sharing of IoT resources, and in this way, physical resources can be virtualized. Furthermore, an IoT-Cloud environment has advantages in terms of availability and efficiency using various devices and protocols. However, issues such as reliability and security are challenging tasks, and many studies in this area are under way. A typical application area of such an IoT-Cloud technology is a smart-grid environment. Power control systems of a smart-grid can be classified into an energy management system (EMS), supervisory control and data acquisition (SCADA) system, and a distribution automation system (DAS). An EMS is a management system that monitors and controls the power system. It consists of a system-operation related optimization program, and conducts optimal system operations by linking with various systems organically. An SCADA system is an automatic control system used in power transmission / transformation systems for equipment control. It monitors and measures data for a variety of power equipment existing in power substations, and provides the corresponding information to the regional control center (RCC) of a metropolitan unit [6]. Finally, a DAS is a system that monitors the field information (status information, current/voltage, occurrence of failure, etc.) for the

power distribution equipment, and when a failure occurs, it reduces the power outage section and power outage time by controlling the automated switch of the failure section. In such a power IoT-Cloud environment, data processing and savings should be conducted in a sufficiently reliable manner when services are received through a connection with various services of a cloud environment, and the confidentiality, integrity, and availability of the data, along with privacy protection, should be guaranteed. In the processes related to cloud services executed on IoT devices, a vulnerability can occur from the device operation. Moreover, risks may occur in the data generated and processed by the devices. Therefore, data processing and movement between IoT-based processing devices at various locations should be processed safely and reliably [7]–[9]. In addition, reliable communication from device objects to the cloud service, as well as safe accessibility and connectivity, should be provided. The security threats that can occur in a power IoT-Cloud environment are classified as shown in Table 1.

TABLE 1. Security threat classification for power IoT-Cloud environment.

Security Threats	Description
Denial of service (DoS) attack	Because power IoT devices have limited computing resources, DoS attacks can occur with a small increase of traffic
Message forgery	Malfunction of a device is induced by forging/falsifying configuration and operation messages of device
Malicious codes	Malicious codes are inserted through software update, etc. such that the device will not operate properly
Firmware manipulation	The information (master encryption key) of firmware is derived and used, or permanent DoS (PDoS) attack is performed
Physical change	When a power IoT such as a smart-meter is placed outside, it becomes a target of physical attack
Control signal change	When control signals such as load control and outage control signals from a power operation system are changed, the entire power IoT is affected
Power usage information change	By changing the power usage information, the load management of the IoT can be affected, which can influence the billing information of the user
Private information exposure	Because personal data contain a variety of information such as personal identification information, billing information, power usage information, and personal behavior information, significant damage may occur when exposed

B. ONTOLOGY-BASED SECURITY CONTEXT REASONING

Context reasoning can be defined as a method for adding understanding, as well as for reasoning new knowledge based on usable context data. Reasoning is an essential function required when solving the incompleteness and uncertainty of unprocessed context data. Ontology-based reasoning executes a function that infers knowledge and facts obtained from the ontology. An ontology is a major semantic technology component used for the modeling of data and is applied to the sharing of a common understanding of an information structure between humans and software agents, domain knowledge analysis, domain knowledge separation from operation knowledge, reutilization of domain knowledge, and the inference of high-level knowledge. An ontology consists of elements such as individuals, properties, classes, relations, and axioms.

In recent years, progress has been made in context-aware services, which provide appropriate services to users by analyzing and learning the information for the surrounding area in an IoT environment. A context-aware service identifies a context by using the surrounding environment information, which can be collected from sensor devices of the IoT system; it then reasons, generates, and provides appropriate services to users. The techniques used for the execution of a context aware service include a statistical method and a method for recognizing the current data and predicting a future state based on machine-learning. Such techniques include rule- and case-based reasoning. Rule-based reasoning generates a service by conducting the reasoning for data that satisfy a certain rule among the input data based on rules between certain data as defined by the user. In contrast, case-based reasoning combines same/similar cases based on past experience to solve a current problem. Furthermore, reasoning techniques that apply supervised learning, unsupervised learning, reinforced learning, and a neural network through machine training are typical examples. Regarding security in a power IoT-Cloud environment, the types of attacks are diverse unlike those of a conventional power grid, and can lead to significant damage at the national scale [10]. To defend against these types of attacks, an integrated and intelligent security technology that applies ontology-based context-aware reasoning is required for clear decision-making and a quick response for attacks occurring continuously in a power IoT-Cloud environment [11].

III. ONTOLOGY-BASED SECURITY CONTEXT REASONING FOR POWER IOT-CLOUD ECURITY SERVICE

A. POWER IOT-CLOUD SECURITY SERVICE FRAMEWORK

Fig. 2 shows a schematic diagram of a power IoT-Cloud security service framework. The proposed system consists of four layers, the details of which are as follows. As Fig. 2 indicates, the IoT management and IoT layer collect security-related information of the power IoT devices, which consist of power IoT log records, a current status analysis module manager, and an IoT sensor data collection module. The corresponding modules receive the sensor security state and security log records from the security context management module to collect data from various heterogeneous IoT sensors [12]. The IoT management and IoT layer send the collected security-related information to the security context management module of the security context conference layer.

The security context conference layer determines the security context by using the security data delivered from the cloud computing layer and the IoT layer. To this end, it uses the context inference module, which uses the information

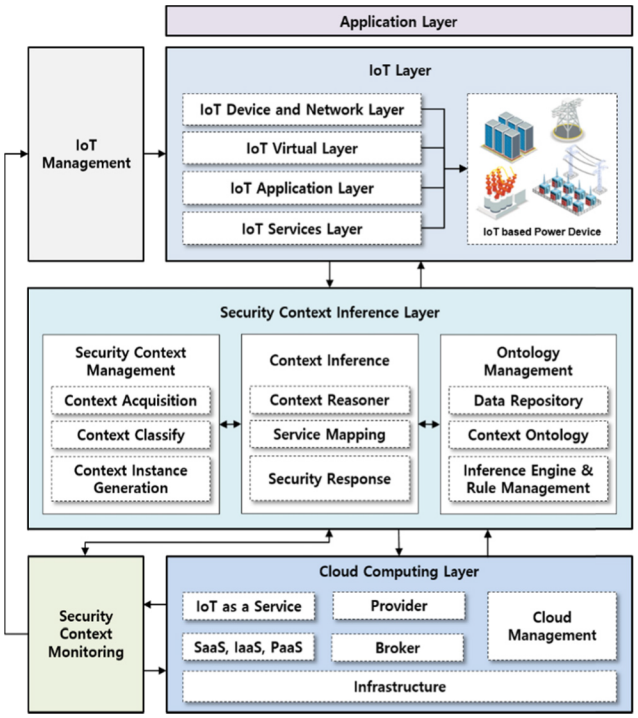

FIGURE 2. Framework of power IoT-Cloud security service.

TABLE 2. Security factors and details of power IoT-Cloud.

Security Factors of Attacks	Security Details
Malicious bot detection and response	Malicious bot distribution server blockage, control of various communication protocols, analysis based on signatures and behaviors, treatment of host infected by malicious bot, quarantine of host infected by malicious bot, removal of malicious bot, blocking zombie PC and C&C server, detection and blockage of abnormal traffic, providing malicious bot detection information, notifying abnormal traffic to administrator
Audit records	Log generation and access history records, setup changes and security function execution records, NTP server time information, server OS time information, query by log generation details, notifying the administrator in advance when the capacity is exceeded, log protection when the capacity is exceeded, log access right restriction, log deletion, and modification control
Identification and authentication	Identification and authentication of administrator, deactivation for a certain time when the administrator authentication fails, locking the account when a user authentication fails, setting up strengthened password rules, masking when inputting/changing a password, error information control when a password fails
Transmitted data protection	Encrypted transmission when sending/receiving data, verification of encryption-related protocol safety
Security management	Security functions, security policy setting, IP restriction for assessing an admin server
Agent protection	Integrity of execution file, integrity of filter driver, recovery function when modified data are discovered, and non-repudiation and integrity are guaranteed

defined in the ontology to determine the security context. The security context management layer is a module that collects security context information, and after generating context information by collecting security data of the IoT devices, it produces a security event in the context inference module. The inference engine and rule management module coverts query generation and security context ontology into a web ontology language (OWL) for the inference of the security context ontology. The context inference module converts the received security context information into a query type, which can be inferred with the ontology. It then infers the security context. For the inference, the context ontology and designed inference rules are referenced. After inferring the security context information, a response method is provided for the security context by providing the security context to the security response module.

B. DEFINITION OF POWER IOT-CLOUD SECURITY CONTEXT AND DESIGN OF ONTOLOGY

Attacks in a power IoT-Cloud environment include an internal system intrusion, network and device vulnerabilities, malicious code infection, and information leakage, and these attacks can be mainly classified into structural, physical, and external attacks [13], [14]. Structural attacks use vulnerabilities of the architectural design of the system, and include attacks using weaknesses of the protocols, authentication process, and system modularization. Physical attacks use the vulnerability of the source codes, and include attacks that take advantage of a SQL injection, a buffer overflow, and other factors [15], [16]. External attacks use programs other than the attack targets, including a Trojan horse, virus, or worm. Such attacks are analyzed and used for the construction of an ontology for security context in a power IoT-Cloud environment. Specific security factors and details are provided in Table 2.

Furthermore, a home energy management system (HEMS), smart meter, smart appliance, access point (AP), and router can be considered for major devices of a power IoT-Cloud environment. These systems that compose the power IoT-Cloud environment consist of various types of power systems ranging from devices that have power transmission functions to those that are used by users that consume electric power. To construct a power security ontology, the classes are defined based on the systems inside the power IoT-Cloud environment. The power security ontology is configured with five levels of classes.

Fig. 3 shows the definitions of seven related domains for the construction of a power security ontology. In conventional smart-grid roadmaps, the lower-level classes are classified using five domains (customer, power grid, service, new regeneration, and transportation), although in the present paper an extended model of this is shown. In the case of the ''power transmission and distribution'' class, because the lower level classes are the same, they are integrated and classified as indicated in Table 3.

Furthermore, a metering system, a lower level class of the operation class, which is a core domain, is defined in Table 4.

The metering system class of Level 3 was classified into two classes, Physical_Access and Network_Access of

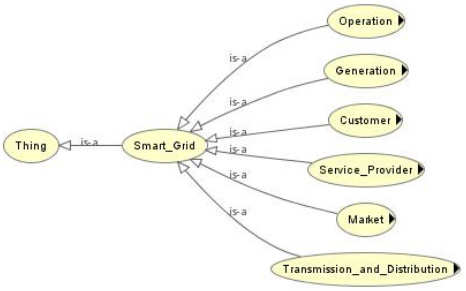

FIGURE 3. Relationship diagram of upper level classes of power security ontology.

TABLE 3. Definition of Levels and Level 3 of power security ontology.

Level	Class	Level	Class
2	Operation	3	Asset_Management, EMS, Metering_System, DMS, MDMS, Distribution_SCADA, WAMPAC, Demand_Response, Transmission_SCADA
2	Generation	3	Generator, Electric_Storage, Market_Service_Interface, Plant_Control_System
2	Customer	3	Energy_Service_Interface, Customer_Equipment, Thermostat Customer_EMS, Appliances, Meter, Customer_Substation
2	Service_ Provider	3	Home_Manager, aggregator, Retail_Energy_Provider, CIS, Billing, Others
2	Market	3	Retailer, Energy_Market_Clearinghouse, Aggregator
2	Transmission_ and_ Distribution	3	Data_Collector, Field_Device, Substation_Controller, Substation_Device

TABLE 4. Partial classes of from Levels 3 to 5 in the power security ontology.

Level	Class	Level	Class	Level	Class
3	Metering_ System	4	Network_Access	5	Application_Protocol_Attack Smart_Meter_Attack Management_Software_Attack ZigBee_Attack
		4	Physical_Access	5	Management_Port_Access Memory_Dump Data_Sniffing

Level 4, and the security attack behaviors were sub-classified as Level 5. Because the ontology classifications are sub-divided, it becomes easier to determine which system has been attacked. Table 5 defines the major properties of the metering system class.

TABLE 5. Property definitions of Metering_System class.

Class	Property
Total	resultIn (result value for a corresponding behavior), behavior (value of behavior appeared), hasType (type for behavior), hasEffect (effect of behavior), hasPurpose (attack goal for behavior)
Network_Access	usedConfig (event registration), usedFileread (device list query), usedFilewrite (device file control), hasRemoteControl (remote device control), hasProtocol (device protocol value), hasRegistrationDate (issue date of behavior information)
Physical_Access	isLocated (location of metering system), hasUserId (user's ID), hasPassword (user's password), has_Key (user's key value), hasLocalControl (local device control), hasRegistrationDate (issue date of behavior information)

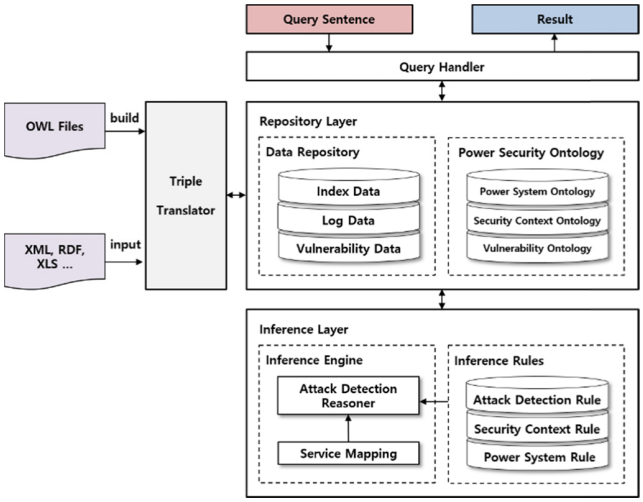

FIGURE 4. Reasoner module.

C. SECURITY CONTEXT INFERENCE MODULE AND RULE DESIGN

In a power IoT-Cloud environment, the security context reasoner module consists of an inference engine and ontology repository. A triple translator, query handler, and reasoner belong to the inference engine and are executed while being linked with the ontology repository. In this paper, Jana, a Java-based rule engine, is used as the inference engine, and initializes the ontology repository or performs the query tasks. The triple translator builds an OWL file in the ontology repository, or changes input files of XML, RDF, and XLS types in a triple structure and saves them in the ontology repository. The reasoner is a module that applies an inference according to the inference rules set up by the user. The query handler composes a query in SPARQL format upon request, and by using a select statement, it infers the security context in the power IoT-Cloud environment. Fig. 4 shows the configuration of a reasoner module.

Designing the security context inference rules is a very important task for recognizing and analyzing security contexts. Attacks applied to the power IoT-Cloud environment are performed using the vulnerabilities of various IoT devices. In this section, therefore, the inference rules designed in SWRL language by classifying the attack behaviors, which use the security vulnerabilities of a power IoT-Cloud environment, in different levels are described. For example, vulnerability inference rules for physical access and network access can be defined as follows based on the attack context information that uses the well-known vulnerabilities of a smart metering system.

- *Physical_Access:* *(?T Memory_Readout_Techniques) ∧(Memory_Readout_Techniques resultIn Memory_Reading) ∧(Memory_Reading resultIn Data_Gathering) => (?T Side_Channel_Attack)*
- *Network_Access:* *(T? behaviour Data_Sniffing) ∧(Data_Sniffing resultIn Packet_Decoding) ∧(Packet_Decoding resultIn Key_Acquisition)∧(Key_Acquisition resultIn Data_Gathering)⇒(?T step Data_Sniffing)*

The attack stage is a stage that acquires relevant information before an attacker attacks a system directly. According to the inference rules, in the case of a hardware access method, the attacker penetrates directly into a smart meter placed outside or through related lines, and after repeatedly conducting the same transaction multiple times, reads the memory and acquires the information. In such a way, the data on the power inside the smart meter can be acquired. During the network attack stage, the encryption key and certificate on the smart meter can be acquired by decoding and analyzing each packet through a data sniffing. The system is accessed using the acquired key. The following shows the inference rule in the system access stage.

- *System_Access:* *(?T behaviour Key_Acquisition) ∧(Key_Acquisition resultIn Data_Gathering)∧(Data_Gathering resultIn System_Access) => (?T Back_Door)*

During the attack stage, when the encryption key and certificate of the relevant user are acquired and analyzed, the attacker accesses the system based on existing vulnerabilities. This stage is defined as the system access stage in this paper. In the system access stage, the attacker accesses the system using the acquired key and user information, and after doing so, the attacker inserts a backdoor for malicious actions so that an attack path will be provided.

The next rule is for the system manipulation stage whereby the attacker who accessed the smart meter system can illegally manipulate the information of meter system. In this stage, the system can be attacked using the power control system, or send manipulated power data usage to the user. Furthermore, this stage provides an environment that can paralyze the power system through the use of well-known Stuxnet or Duqu attacks.

- *Remote_Access:* *(?T behaviour Data_Gathering) ∧(Data_Gathering resultIn System_Access) ∧(System_Access resultIn System_Control) => (?T REMOTE ACCESS)*

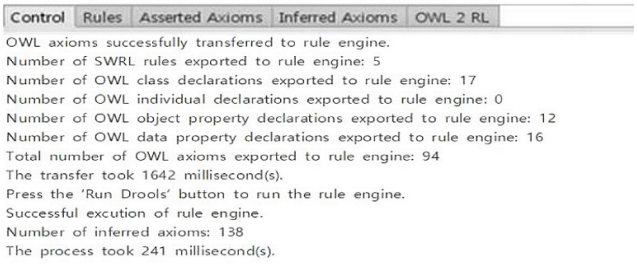

FIGURE 5. Execution results of SWRL inference rules.

TABLE 6. Network attack context extractions and class definitions in the power IoT-Cloud environment.

Attack Sequence	Attack Context	Related Class
Attack Sequence 1	Accesses the system after stealing packets	System_Access
Attack Sequence 2	Failure of smart meter operation at the user's home	DDoS_Attack, ExIPPacketSize
Attack Sequence 3	Virus propagation and infection in nearby devices	Various_Attack, Various_Infection
Attack Sequence 4	Operation halts of nearby smart meter systems	System_Shutdown

IV. EXPERIMENT AND EVALUATION

In this section, the security context reasoning service in a power IoT-Cloud environment evaluated experimentally is described. An attack applied to a smart meter is used as an example during the security context reasoning test for attack detection in the power IoT-Cloud environment. The most common context among smart meter security contexts is that, when a system operation failure occurs in a smart meter device system for an unknown reason, system shutdown damage occurs in other nearby systems. Since the power system environment uses bi-directional communication, an attack using a vulnerability of system should be suspected for the network attack, and the relevant environment should be inspected promptly. Fig. 6 classifies such attack contexts into different stages and shows the sub-classes.

The system access context after stealing packets, which is a first attack context, is defined as Attack Sequence 1 because

TABLE 7. Inference rules of attack context detection.

Attack Context	Rules
Network_Access	(T? behaviour Data_Sniffing) ∧ (Data_Sniffing resultIn Packet_Decoding) ∧ (Packet_Decoding resultIn Key_Acquisition) ∧ (Key_Acquisition resultIn Data_Gathering) ⇒ (?T step Data_Sniffing)
System_Access	(?T behaviour Key_Acquisition) ∧ (Key_Acquisition resultIn Data_Gathering) ∧ (Data_Gathering resultIn System_Access) => (?T Back_Door)
Remote_Access	(?T behaviour Data_Gathering) ∧ (Data_Gathering resultIn System_Access) ∧ (System_Access resultIn System_Control) => (?T REMOTE ACCESS)
Movement	(?T behaviour Back_Door) ∧ (Back_Door resultIn Adjacent_System) ∧ (Adjacent_System resultIn Malware_Drop) => (?T Various_Attack)
ShutDown	(?T behaviour Various_Attack) ∧ (Various_Attack resultIn System_Access) ∧ (System_Access resultIn System_Control) ∧ (System_Control resultIn Destruction) => (?T System_Shutdown)

the system can be accessed only by stealing packets through network access. The second attack context, i.e., operation failure of the smart meter at the power user's home, is a context for checking whether the attacker has accessed the system. It is a context whereby the system operation failure is induced by decreasing the system resources or sending large-sized packets continuously upon intention through a DDoS attack. The third attack context, i.e., virus propagation and infection in nearby devices, is a context whereby the attacker spreads a virus in nearby devices and conducts malicious activities as originally intended after successfully accessing the system in the second attack context. In addition, the attacker can insert a backdoor to create a path to continuously access the system. The fourth attack context, i.e., the operation halts of nearby smart meter system, is a context that induces large-scale power outage of infected systems by sending a shutdown control command. After extracting the attack contexts based on the aforementioned attack scenario, the attack context detection inference rules are composed, as shown in Table 7, through the design rules composed for each stage using the semantic web rule language (SWRL).

As a result of executing SWRL-based inference rules in the ontology inference engine, as shown in in Fig. 5, the corresponding attacks can be successfully detected using the presented inference rules.

Table 8 shows the inference rules designed based on the security context ontology for a variety of attacks of power an IoT-Cloud environment, and their attack detection rates.

TABLE 8. Inference recognition rate based on attack context in a power IoT-Cloud environment.

Attack Pattern	Attack Context and Inference Rules	Attack Detection Rate
Memory Dump	An attacker steals information and damages a system by accessing memory dump	87.5%
	(?T behaviour Memory_Dump_Access) ∧ (Memory_Dump_Access resultIn usedFileread) ∧ (usedFileread resultIn Buffer_Overflow) ∧ (Buffer_Overflow resultIn Key_Acquisition) ∧ (Key_Acquisition resultIn System_Damaged)	
Port Access	Extraction of important information such as network key and metering information	91.1%
	(?T behaviour Port_Access) ∧ (Port_Access resultIn Routing_Attack) ∧ (Routing_Attack resultIn Session_Hijacking) ∧ (Session_Hijacking resultIn Meter_Data)	
Data Sniffing	Extracting user information and encryption key information	92.5%
	(T? behaviour Data_Sniffing) ∧ (Data_Sniffing resultIn Packet_Decoding) ∧ (Packet_Decoding resultIn Key_Acquisition) ∧ (Key_Acquisition resultIn Data_Gathering)	
Software Attack	Malicious firmware update is performed by attacking vulnerabilities of firmware	86.1%
	(?T behaviour Firmware_Attack) ∧ (Firmware_Attack resultIn usedConfig) ∧ (usedConfig resultIn File_Update)	
Protocol Attack	Attack through re-transmission after extracting relevant packets	78.4%
	(?T behaviour Intercept_Packet) ∧ (Intercept_Packet resultIn extraction_Packet) ∧ (extraction_Packet resultIn Relay_Message)	
ZigBee Attack	Security network discovery, device identification attack, and pack blocking attack	91.5%
	(?T behaviour Network_Access) ∧ (Network_Access resultIn Traffic_Capture) ∧ (Traffic_Capture resultIn Traffic_Save)	

The inference rules were defined based on a pattern for the security contexts that can occur in a power IoT-Cloud environment, and the attack detection rates were measured. Because the system attack methods are extremely diverse in a large-scale power IoT-Cloud environment, it is difficult to detect the attacks using a pattern-based probabilistic detection method. Therefore, the security context inference methodology proposed in this study is significant as a solution to this. Furthermore, through a combination of defined inference rules, it is possible to respond to more complex attack contexts.

V. CONCLUSION

This paper analyzed the security vulnerabilities of power systems in a power IoT-Cloud environment, modeled the security context ontology, and defined the security context inference rules. Furthermore, a suitable power IoT security service framework was proposed that can be used in a power IoT-Cloud environment, and implements a security mechanism that can operate efficiently in such an environment. To design the security context ontology proposed in this paper, vulnerabilities of the major solutions and systems were collected and analyzed respectively for the power systems of a power IoT-Cloud environment, and based on these vulnerabilities, focus was placed on the security context ontology modeling. Moreover, the attack patterns in the power IoT-Cloud environment, and the attack-related vulnerabilities of each system in the major domains, were analyzed. A vulnerability-based attack context inference methodology was also proposed.

For the experiments conducted in this study, attack context scenarios that can occur commonly were created using an example of a smart meter, an essential device in a power system; inference rules were then composed to check the path of an attack that uses the vulnerabilities of the smart meter system at each stage. As a result, a high level of attack detection was confirmed through the inference rules. The proposed security context reasoning method can be applied to new security attack detections by expanding the security context inference rules. However, an understanding of complex power systems is essential, and it is necessary to design more detailed vulnerability categories for each power system to be able to expand the systems for diverse security attack contexts. In addition, a process of defining inference rules for such contexts is required.

REFERENCES

[1] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generat. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.

[2] C. A. Kamienski, F. F. Borelli, G. O. Biondi, I. Pinheiro, I. D. Zyrianoff, and M. Jentsch, "Context design and tracking for IoT-based energy management in smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 687–695, Apr. 2018.

[3] C. Xiaqin, L. Le, Q. Feng, X. Zhong, L. Junxiang, and X. Tianwei, "Intelligent location and analysis of power grid fault trip based on multi-source data," *Energy Procedia*, vol. 141, pp. 580–586, Dec. 2017.

[4] L. Liang, "Electric security data integration framework based on ontology reasoning," *Procedia Comput. Sci.*, vol. 139, pp. 583–587, Jan. 2018.

[5] S. Zander, N. Merkle, and M. Frank, "Enhancing the utilization of IoT devices using ontological semantics and reasoning," *Procedia Comput. Sci.*, vol. 98, pp. 87–90, Jan. 2016.

[6] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," in *Proc. 1st Annu. Conf. Res. Inf. Technol.*, Oct. 2012, pp. 51–56.

[7] C. Choi, C. Esposito, H. Wang, Z. Liu, and J. Choi, "Intelligent power equipment management based on distributed context-aware inference in smart cities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 212–217, Jul. 2018.

[8] S. Howell, Y. Rezgui, J.-L. Hippolyte, B. Jayan, H. Li, "Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources," *Renew. Sustain. Energy Rev.*, vol. 77, pp. 193–214, Sep. 2017.

[9] C. Kamienski, M. Jentsch, M. Eisenhauer, J. Kiljander, E. Ferrera, P. Rosengren, J. Thestrup, E. Souto, W. S. Andrade, and D. Sadok, "Application development for the Internet of Things: A context-aware mixed criticality systems development platform," *Comput. Commun.*, vol. 104, pp. 1–16, May 2017.

[10] Y. Huang and X. Zhou, "The study of power grid generalized data management model based on ontology theory," *Autom. Electr. Power Syst.*, vol. 38, no. 9, pp. 114–118, May 2014.

[11] M. Roopaei, P. Rad, and K. R. Choo, "Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 10–15, Jan. 2017.

[12] Y. Huang and X. Zhou, "Knowledge model for electric power big data based on ontology and semantic Web," *CSEE J. Power Energy Syst.*, vol. 1, no. 1, pp. 19–27, May 2015.

[13] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, and R. Jardim-Goncalves, "An ontology-based cybersecurity framework for the Internet of Things," *Sensors*, vol. 18, no. 9, p. 3053, Sep. 2018.

[14] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046–21056, 2017.

[15] Y. Pradeep, S. A. Khaparde, and R. K. Joshi, "High level event ontology for multiarea power system," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 193–202, Mar. 2012.

[16] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.