Cyber security framework for Internet of Things-based Energy Internet

Abubakar Sadiq Sani, Dong Yuan, Jiong Jin, Longxiang Gao, Shui Yu,
Zhao Yang Dong

PII: S0167-739X(17)30660-X
DOI: https://doi.org/10.1016/j.future.2018.01.029
Reference: FUTURE 3936

To appear in: *Future Generation Computer Systems*

Received date : 15 April 2017
Revised date : 21 November 2017
Accepted date : 15 January 2018

Cyber Security Framework for Internet of Things-Based Energy Internet

Abubakar Sadiq Sani[a], Dong Yuan[a], Jiong Jin[b], Longxiang Gao[c], Shui Yu[c], Zhao Yang Dong[d]

[a] *The University of Sydney, New South Wales, Australia*
[b] *Swinburne University of Technology, Victoria, Australia*
[c] *Deakin University, Victoria, Australia*
[d] *The University of New South Wales, New South Wales, Australia*

Abstract

With the significant improvement in deployment of Internet of Things (IoT) into the smart grid infrastructure, the demand for cyber security is rapidly growing. The Energy Internet (EI) also known as the integrated internet-based smart grid and energy resources inherits all the security vulnerabilities of the existing smart grid. The security structure of the smart grid has become inadequate in meeting the security needs of energy domains in the 21st century. In this paper, we propose a cyber security framework capable of providing adequate security and privacy, and supporting efficient energy management in the EI. The proposed framework uses an identity-based security mechanism (I-ICAAAN), a secure communication protocol and an Intelligent Security System for Energy Management (ISSEM) to certify security and privacy in the EI. Nash Equilibrium solution of game theory is applied for the evaluation of our proposed ISSEM based on security events allocation. The formal verification and theoretical analysis show that our proposed framework provides security and privacy improvement for IoT-based EI.

Keywords: Energy Internet, Cyber Security, IoT, I-ICAAAN, Secure Communication

1. Introduction

Security attacks on smart grid have increased over the last few years. These attacks have led to great economic losses and increase in environmental concerns. The current security posture of the smart grid is inadequate to address all its existing and emerging security attacks. The concept and adoption of Energy Internet (EI) will significantly improve the security of the smart grid. EI is proposed as an integrated platform with multidirectional communication and power flow mechanisms designed for improvement of the smart grid. The IoT technologies are used to collect and analyse real-time data for intelligent energy management. EI ensures that the energy domains such as generation, transmission, distribution, operations, service provider, markets, end-users and regulators are seamlessly integrated. It enables the gradual transition from non-renewable to renewable energy sources [1] [2] [3] which supports energy management initiatives like environmental and economic efficiencies. The concept of EI can also be referred to as a software platform for controlling, monitoring and managing the entire smart grid, with interconnectivity orientation amongst all power systems [4]. It provides new energy efficiencies not limited to intelligent energy management, automatic redirection and adjustment of energy usage, energy security, asset degradation control and availability of smart energy choices to customers. EI is envisaged as the technology to transform the smart grid into a smarter grid via improved technological advancement with the support of IoT for the entire future smart grid system.

The IoT is a key enabler for the energy domains [5] in which sensing and actuating are major features of many assets in order to increase operational and communication efficiencies. The capabilities of IoT in EI for adequate energy management supports the efficient detection of security vulnerabilities and attacks. However, due to the complexity nature of the IoT, it is very challenging to design a fully secure and efficient framework to detects and prevents security vulnerabilities and attacks in EI. One of the main features of EI is the ability to use IoT to control and monitor all the activities and functionalities of the smart grid [6]. While the research about EI security has just begun, the importance of security software framework in the energy sector is becoming more prominent. The security attacks on assets, data, network, users and applications are huge challenges for the EI. These security attacks and other challenges such as risk management and network assurance are major security problems that we need to study and solve.

In this paper, we propose a cyber security framework for the IoT-based EI taking into account the existing security concerns in the smart grid. The proposed framework comprises of an identity-based security mechanism (I-ICAAAN), secure communication protocol and an Intelligent Security System for Energy Management (ISSEM). I-ICAAAN represents integrity, confidentiality, availability, authenticity, authorisation and nonrepudiation security parameters. It integrates the security parameters to support components, data and events in EI, which is capable of preventing security vulnerabilities and attacks, and addressing the security misconfiguration and session mismanagement concerns facing the smart grid thereby providing end-to-end security in EI. The secure communication protocol provides adequate secure data exchange in EI, and it uses the I-ICAAAN for communication amongst all components. The ISSEM is used for assessing and modelling the security status of the EI. An Intelligent Security Unit for Energy Management (ISUEM) that is controlled by the ISSEM is embedded in an energy management device called Energy Router for assessing the security behaviours of the energy components as propose in this paper. The proposed framework will help to mitigate security concerns in the existing EI architecture presented in [2] [3] [7] [8] [9] and evolutionalized the existing security parameters in place to secure the smart grid.

Our main contributions are: 1) identifying security attacks in the smart grid; 2) proposing I-ICAAAN that takes into account various security parameters required for security and privacy in the EI; 3) presenting a secure communication protocol that supports secure exchange of data and prevents various security attacks in EI; 4) proposing ISSEM that takes into account an ISUEM to further improve the security capabilities in the energy router and EI in general; and 5) proposing a cyber security framework that utilises the I-ICAAAN, secure communication protocol and ISSEM to address critical security challenges of analysing and solving complex smart grid vulnerabilities at scale. The I-ICAAAN provides security and privacy platform for the EI. Identification and authentication security parameters are utilised by default in order to certify and register all components in EI. While the I-ICAAAN is primarily evaluated using theoretical analysis, the secure communication protocol is validated using an Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The ISSEM is assessed and evaluated using Nash Equilibrum since it exhibits properties to analyze the outcome of interaction amongst several players.

The rest of this paper is organized as follows. In Section II, we discuss some approaches and schemes that have been presented for the security of EI and smart grid. Section III describes the EI architecture and its security requirements. Section IV presents our proposed framework. The analysis of our proposed framework, and its comparison with existing related schemes are presented in Section V. Finally, we present our concluding remarks and future research directions in Section VI.

2. Related Works

Cyber Security concerns usually arise in many areas of smart grid and EI [3]. Multiple security and privacy solutions had been proposed to prevent security vulnerabilities and attacks in the smart grid depending on the architecture in used. These solutions have been described in [14] [15] [16] [17] [18] and are mainly based on the use of Q-learning based vulnerability analysis approach [14], dependable framework and taxonomies for energy big data analytics and security [15], Merkle-tree based handshaking scheme [16], authentication and authorisation scheme [17], and virtual ring architecture for privacy protection [18]. Some research focus on security attacks, such as Denial of Service (DoS) attack [19], false data attack [20], Man-In-The-Middle (MITM) attack [21], bad data injection attack [22], cyber physical attacks [23] and data integrity attacks [24]. However, cyber security concerns and vulnerabilities such as weak security configuration and session mismanagement, arising from the smart grid architectures cyber security design stage have not been well investigated. These security issues exist due to weak security design and growing security concerns from the smart grid architecture.

Minoli et al. [10] presented the importance of IoT in smart grid and physical security, and IoT-based systems support for security and energy management, and then offered some technical opportunities on the deployment limitation issues and disjointed cybersecurity solutions currently facing IoT utilization. Yang et al. [11] recognized smart grid as an important form of IoT applications that is vulnerable to cyber-attacks such as contamination attacks and data integrity attacks that can disrupt smart grid operations and cause energy loss and further damaging impacts. Yang et al. [11] further proposed a Gaussian-mixture model-based detection scheme to mitigate the data integrity attacks. While the solutions presented in [10] and [11] can mitigate security attacks in the smart grid, they are inadequate to meet the security requirements of the EI.

Xu et al. [7] presented the importance of communication security in the energy router in order to prevent unauthorised users from intercepting any information during communication and to ensure that falsified information can be detected and discarded. However, the architectural design of the energy router presented in [7] is vulnerable to data, network and asset security threats and issues. The structure of the EI presented in [2] lacks a cyber security interface for energy and information flows through the use of Energy Local Area Network (Energy LAN) and energy router its core equipment. While serious need for research on the protection of EI is proposed in [2], a secure communication protocol for data exchange in EI is required for effective energy operation, production and consumption.

The authors of [9] relate the communication challenges in EI to reliability and security, and propose the need for many researches to help in resolving these communication challenges in other to ensure system reliability and security. Despite the proposed parameters for smart grid security in [12], security during the smart grid communication cannot be guaranteed. The authors in [12] proposed the need for future research on the existing smart grid security standard. Shapsough et al. [1] explained the functions of availability, integrity, confidentiality, authentication, authorisation and nonrepudiation as the security requirements and objectives of the smart grid. However, the security parameters presented in [1] are not integrated and they lack a cyber security design that meets the end-to-end security requirements of the smart grid.

In [13], the authors presented the cybersecurity challenges for Cyber-Physical Systems (CPS) and urged that new architectures and techniques are required to ensure the integrity, confidentiality and availability of data as well as protection of users and assets. The CPS comprise of cyber systems and physical systems used for integrating sensing and intelligence to the power networks [13]. More specific to CPS security attacks, [25] proposed a layered approach for evaluating risk of physical power applications security and cyber infrastructure security. Their work was focused on risk and operational modelling, and did not capture the cyber-physical network security. The process of moving control systems such as SCADA system to a cloud-based environment is one of the tasks associated with the EI, however, security vulnerabilities and attacks must be addressed.

It is worth noting that many extensive research already articulated the need for security and privacy solutions for the EI [2] [3] [7] [9]. However, we found that many of the existing approaches in the literature are not suitable to meet the security and privacy of the EI. A simple comparison of security parameters amongst various existing related approaches and schemes is presented in Table 1. This table shows the security parameters that are utilised in these approaches and schemes.

Table 1: Comparison of Security Parameters

Security Parameters	Shapsough et al. [1]	Minoli et al. [10]	Yang et al. [11]	Elgargouri et al. [12]	Yu et al. [13]
Identification	×	✓	×	✓	×
Authentication	✓	✓	✓	✓	×
Integrity	✓	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓	✓
Availability	✓	✓	×	✓	✓
Authenticity	×	×	×	×	×
Authorisation	✓	✓	✓	×	×
Nonrepudiation	✓	×	×	×	×

3. Energy Internet Architecture and Security Requirements

According to Jeremy Rifkin [4], EI represents a new convergence between communication, energy and internet. In this section, we first examine a simple EI architecture from which we identify and present the EI security requirements. The EI architecture is made up elements that are capable of providing security and privacy to components, data and events in EI thereby supporting energy management.

3.1. Energy Internet Architecture

As shown in Figure 1 [26], we describe the EI architecture to ensure its effectiveness in securing and maintaining privacy across all its components. It should be noted that IoT [27] serves as the underlying element that supports the EI architecture. We present the interconnected elements of the EI architecture, which rely on the IoT for connection and interaction with one another. These elements include: 1) Cyber Systems Layer; 2) Energy Layer; 3) Cyber Security Model; and 4) Secure Communication Model. These elements contribute to the security of the EI. Brief descriptions of the elements are given below:

3.1.1. Cyber Systems Layer

This element is responsible for providing, overseeing and monitoring the cyber systems across the EI. Two major supporting technologies of this element are Supervisory Control and Data Acquisition (SCADA) system and Geographic Information System (GIS). The SCADA system is used for monitoring and controlling operations in EI. Using IoT-based SCADA provides

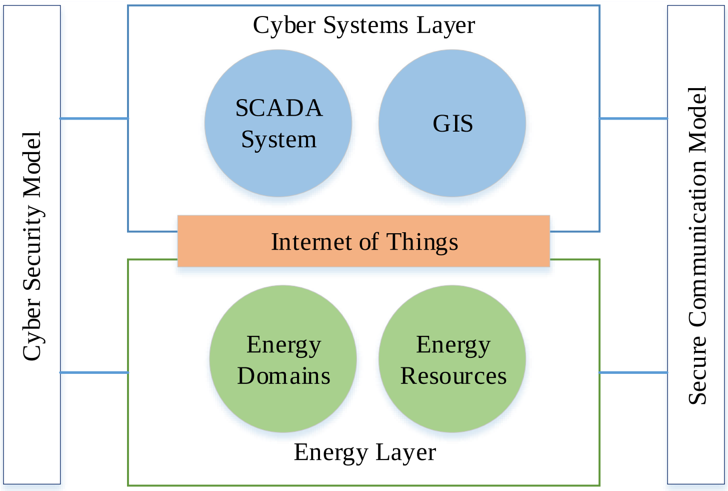


Figure 1: Energy Internet Architecture

improved monitoring and timely decision making in the smart grid [28]. The GIS is used for analysing and processing real-time geographic data to enhance management of energy, and reduce maintenance cost and time [29] [30]. Real-time data from the grid are displayed by the GIS to optimize the performance of the smart grid network [30] [31]. IoT is characterised by energy efficiency [32] [33] and considered as an enabler responsible for providing all connections and interactions that are utilised by these supporting technologies and other elements in the EI. The changing resource constraints such as system resources, operations and performance in Information and Communication Technologies (ICT) have been addressed by IoT for adequate decision making and support [34], thereby preventing any negative impact on the EI architecture. The proposed framework will assist in providing an end-to-end security and privacy to this layer for efficient energy management support.

3.1.2. Energy Layer

This element is responsible for energy management across the energy domains and energy resources [35] of the EI. With the help of IoT, the energy layer is managed in a smart and intelligent fashion. In this paper, we use the smart grid energy domains and introduced three additional entities to support the security and privacy of the EI. These additional entities include: 1) regulator/legal; 2) Cyber Security Change Authority (CSCA); and 3) Cyber Security Assurance Authority (CSAA). The regulator/legal will monitor, enforce and automate energy compliance across the energy domains. Both the CSCA and CSAA are cyber security authorities of the EI. The CSCA is a cyber security authority assigned to authorise and deal with change specifications within the agreements made on cyber security. It is assigned collectively by the energy domains, excluding the CSAA. The agreement is made by the concerned/associated domains (including regulators/legal and excluding CSAA). The CSAA is presented as an entity assigned to monitor the cyber security performance and changes associated with the EI. It is assigned collectively by the energy domains, excluding the CSCA. In addition, one of the energy components utilised by the EI architecture is the energy router which is presented as a concept in energy internet that controls energy flow and information exchange [7]. The energy router uses a communication module for communication amongst power components [7]. Thus, the energy router is utilised in the proposed secure communication model. As presented in Figure 1, energy resources represent the sources and storage of energy. It is sub-divided into the following: 1) renewable energy sources (high rates); 2) non-renewable energy sources (low rates which will be gradually replaced by the renewable energy sources with the help of IoT and EI); and 3) energy storage. The renewable energy sources include wind, solar, rain, waves, tides and geothermal heat while non-renewable energy sources include petroleum, coal and natural gas. Furthermore, IoT ensures that all energy sources are inter-connected for efficient energy management [36].

3.1.3. Cyber Security Model

This element provides end-to-end security and privacy to all layers in the EI. It models and assesses the relationship and dependencies between Functional Security Area (FSA) and Logical Security Area (LSA) of the EI as shown in Figure 2. The emergence of IoT enables the adoption of an extensive approach to cybersecurity for privacy and security improvement in smart grid [37]. With the support of IoT, the FSA interacts with the LSA in real-time to improve energy management. Major entities in FSA are briefly described as follows.

- Asset: This consists of all the energy infrastructure.
- Data: This represents set of values and information.

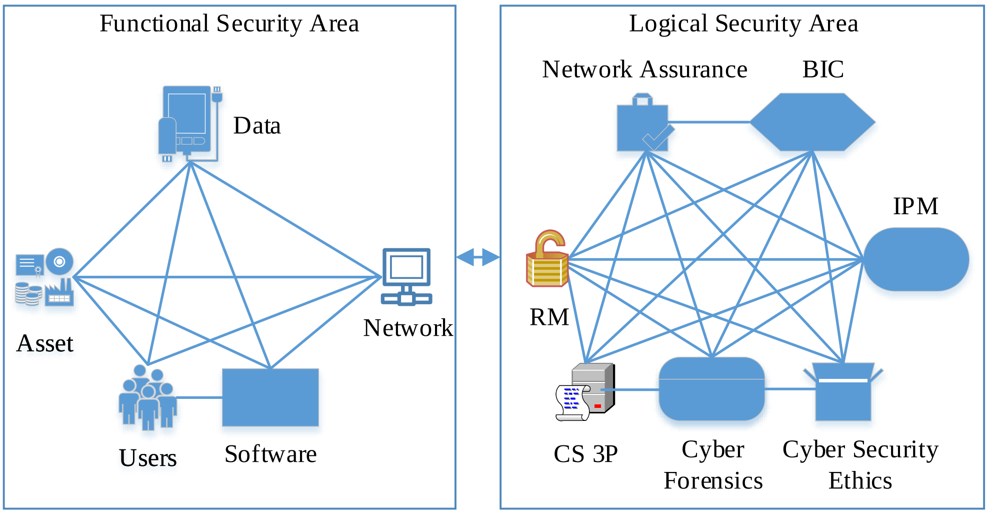


Figure 2: Cyber Security Model. Abbreviations: RM - Risk Management, BIC - Business Information Continuity, IPM - Incident and Problem Management, CS 3P - Cyber Security Policies, Planning and Practices.

- Network: This provides the pathway for connection, communication and services.
- Software: This represents energy applications and programs.
- Users: These are energy operators and customers.

The LSA normally contains the following entities.

- Risk Management (RM): This is used for identifying, assessing, prioritising and controlling security threats.
- Network Assurance: This provides network insights to reduce any vulnerabilities or attacks.
- Business Information Continuity (BIC): This presents control plan for vulnerabilities and threats
- Incident and Problem Management (IPM): These represent scalable proactive processes towards cyber security incidents, with preparation, detection, analysis, containment, eradication and recovery techniques.

- Cyber Security Ethics: This consists of principles for security, privacy, trust, safety and usability across the EI.
- Cyber Forensics: This is used for detection, reporting and providing evidence of security vulnerabilities and attacks across the EI.
- Cyber Security Policies, Planning and Practices (Cyber Security 3P): These represent security guidelines, processes, needs and procedures across the EI.

3.1.4. Secure Communication Model

EI depends on communication to coordinate its entire architecture. Given the variety of communication models available in the smart grid, a secure communication model is presented to ensure end-to-end secure data exchange in EI. Figure 3 shows a simple secure communication model for EI, which comprises of the control centre premises and cyber-energy premises. As IoT has pave the way for communication between components without any involvement of human [38], all premises are always reachable. The key performance indicators for communication in EI include reliability, availability, security and maintainability. The secure communication model provides the security and privacy considerations required to ensure the reliability, availability, security and maintainability of communication in the EI. One of the key considerations for EI architecture is end-to-end secure communication where all components, data and events in the EI are considered very critical in order to avoid any form of security attacks such as DoS attack, replay attack, MITM attack, impersonation attack, Sybil attack, false data injection attack and repudiation attack. Additionally, the secure communication model provides communication security to the energy router to ensure end-to-end secure energy flow in EI. Brief descriptions of the major components in the secure communication model are given below.

- Intrusion Detection System (IDS): This is either a hardware or software component used for detecting malicious activities during communication and operations in EI. The IDS is utilised as additional component to defend against potential security vulnerabilities and attacks on IoT-based applications [39].
- Firewall: This could be a hardware device or software system capable of monitoring and controlling network traffic based on the security rules

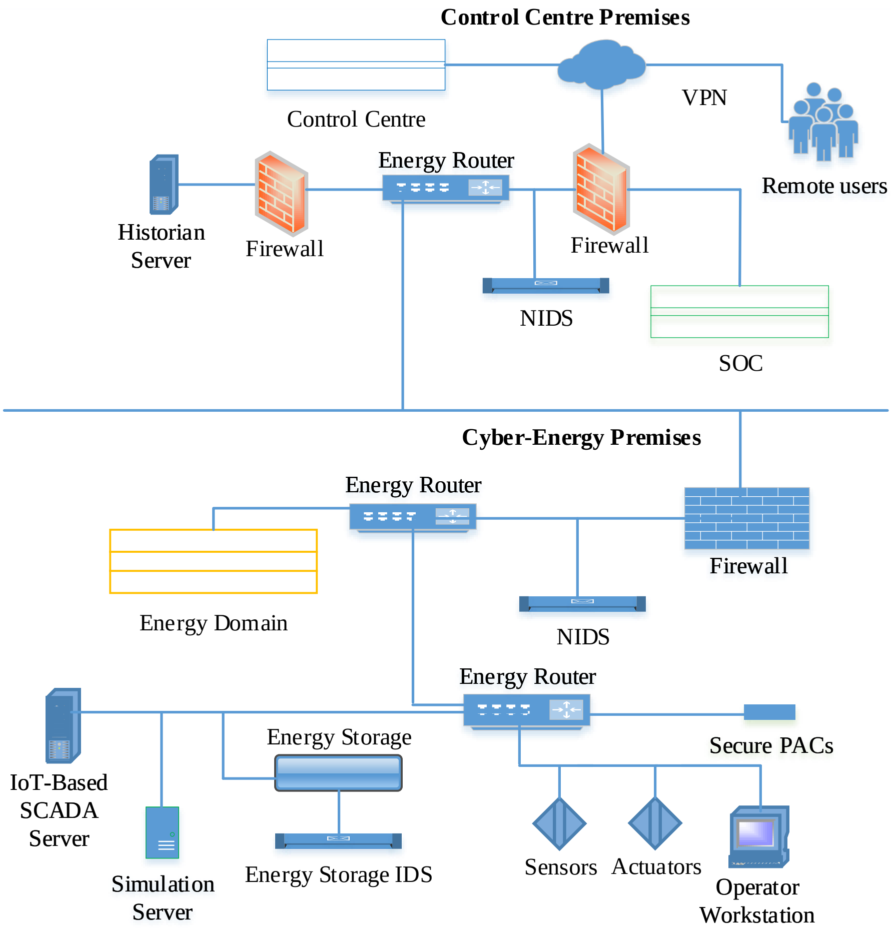


Figure 3: Secure Communication Model. Abbreviations: VPN - Virtual Private Network, NIDS- Network Intrusion Detection System, SOC - Security Operation Centre, IDS - Intrusion Detection System, Secure PACs - Secure Programmable Automation Controllers.

that support effective energy management. Due to the sensitivity of huge amount of data on components and events collected by IoT in any environment, a firewall is used to provide access control and support communication security [40].

- Historian Server: This is a corporate server with enterprise resources/data to support energy management. In this paper, the historian server is deployed to support data security in EI.

- Secure Programmable Authomation Controllers (Secure PACs): These combine the functions of Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) in a secure manner. They act as local control systems supporting the SCADA system or remote controller for energy applications. IoT supports the use of PACs in the smart grid automation [41].

- Simulation Server: This is a virtual operational server imitating the operations of the real systems. It simulates the energy environment for security investigation and testing.

- Sensors and Actuators: These are devices that support the energy environment for advanced connections and interactions. These components are extensively utilised by IoT [42] [43] [44].

3.2. Energy Internet Security Requirements

According to the European Network and Information Security Agency [45], the cyber security requirements for the smart grid include confidentiality, integrity and availability of data and systems. In addition, according to the National Institute of Standards and Technology (NIST) of the United States, security objectives of smart grid data, performance and information systems include confidentiality, integrity and availability of data and information system [35]. Due to the presence of IoT in the smart grid, CIA are not adequate to represent the security parameters of the smart grid [37]. Thus, the cyber security framework for the EI should meet the following security requirements.

- Integrity: This ensures that data and systems are prevented from unauthorised modification by adversaries or unauthorised components. Integrity is considered as one of the important security features in IoT [46].

- Confidentiality: This ensures that data and systems are prevented from unauthorised read access or eavesdropping. To protect data in IoT, confidentiality must be met [46]. In addition, confidentiality is a basic cyber security requirements in IoT [47].

- Availability: EI data and systems are functional and accessible by genuine components. One of the objectives of IoT is to increase system availability [28] [46].

- Authorisation: This ensures that permission is given to authorised components before any event is carried out. Authorisation is presented as a cyber security requirement for granting access to IoT networks in [47].
- Authenticity: This ensures that all authorised components are genuine and can prevent against user impersonation. Authenticity is one of the security goals used for preventing security attacks in IoT [48].
- Nonrepudiation: This ensures that components cannot deny events they carried out. This will further ensure that all events by authorised components and failed-attempts by unauthorised components or adversaries are tracked and recorded for adequate security analysis and forecast. Nonrepudiation is considered as a cyber security requirement that provides proof of entities behaviours in IoT networks [47].

The I-ICAAAN utilises all the aforementioned security parameters to tackle security vulnerabilities and attacks in the EI.

4. Cyber Security Framework for Energy Internet

In this section, we present the proposed cyber security framework for IoT-based EI which includes the composition of the following: 1) I-ICAAAN; 2) a secure communication protocol; and 3) ISSEM. We introduce I-ICAAAN and build a secure communication protocol based on I-ICAAAN, and then we propose a system, ISSEM, that utilises the secure communication protocol.

4.1. Identity-based Security Mechanism (I-ICAAAN)

I-ICAAAN uses the combination of integrity (*int*), confidentiality (*con*), availability (*ava*), authenticity (*aut*), authorisation (*auo*) and nonrepudiation (*nor*) security parameters to provide and certify the security and privacy of components, data and events in the EI. It is proposed to address the security concerns in the EI. The energy domains can connect and interact with the energy resources or any other part of the EI based on the I-ICAAAN. Moreover, the EI architecture is set to make use of identity-based function to aggregate an event or component's request. A proposition is presented to show how the I-ICAAAN handles the security parameters and supports secure communication in EI. The notations used in this paper are presented in Table 2.

Table 2: Notations and Meanings

Notations	Meanings
T_{SE1}	Timestamp of sensor $SE1$
N_{SE1}	Nonce of sensor $SE1$
ID_{SE1}	Identity of sensor $SE1$
M_{SE1}	Message by sensor $SE1$
K	shared secret key between components
SP	Security and Privacy of a component
$CS(.)$	Cipher-based MAC signing operation
$CV(.)$	Cipher-based MAC verification operation
$G_{SE1.SE2}$	MAC Tag between sensor $SE1$ and sensor $SE2$
$E(.)$	Encryption Operation
$D(.)$	Decryption Operation
S_i	Strategy set for player i
f_i	Playoff function of player i
t_n^a	Attack action by an attacker A
C_n^A	Cost of attacker A implementing an attack action
IC_n^{ta}	TA action based on I-ICAAAN
C_n^{TA}	Cost of TA implementing the I-ICAAAN action
C_i^{ta}	Cost of TA supporting I-ICAAAN communication
R_A	Total number of resources available to attacker A
C_A	Cost of the attacker A to perform an attack action

Proposition 1:. I-ICAAAN provides the security and privacy that supports secure communication in EI.

Proof:. Let *int*, *con*, *ava*, *aut*, *auo*, *nor* be security parameters such that they connect to each other for adequate security and privacy in EI. Then we have: $SP = \mathit{int} \wedge \mathit{con} \wedge \mathit{ava} \wedge \mathit{aut} \wedge \mathit{auo} \wedge \mathit{nor}$ for presenting the security and privacy of any component in EI (this shows that all the security parameters must be met by any component in order to achieve security and privacy in EI).

Failure of any security parameters $Int, Con, Ava, Aut, Auo, Nor$ cannot guarantee security and privacy (including secure communication) in EI. One of the major issues in IoT is lack of identification standard for objects [49]. The proposed I-ICAAAN will assist in supporting the identification of objects in EI, and can further be considered as a security identification standard in energy management.

4.2. Secure Communication Protocol

This provides secure end-to-end data exchange between components in the EI. It is designed with the support of Cipher-based Message Authentication Code (CMAC) [50] and other cryptpographic operations, taking into considerations the I-ICAAAN. We consider the secure communication model presented in this work. We assume that a trusted authority, TA, in the energy domains is responsible for identifying and authenticating every component in EI. Suppose a Sensor, $SE1$, wants to exchange data with another Sensor, $SE2$, we assume that: 1) $SE1$ and $SE2$ have two shared secret keys K_1 and K_2 to support the secure communication between them (these shared secret keys are only known by $SE1$ and $SE2$); 2) $SE1$ and $SE2$ have knowledge of the CMAC signing operation, $CS(.)$, CMAC verification operation, $CV(.)$, encryption operation, $E(.)$, decryption operation, $D(.)$, and other operations that are made available by the TA. The steps below represent the secure communication between $SE1$ and $SE2$ utilising the proposed protocol:

- Step 1: $SE1$ encrypts a message, M_{SE1}, with K_1 and use $CS(.)$ that takes the encrypted message, $E(M_{SE1})_{K_1}$, and K_2 to produce a MAC tag, $G_{SE1.SE2}$. Then, $SE1$ joins $G_{SE1.SE2}$ to $E(M_{SE1})_{K_1}$ and send to $SE2$. Along with the message, M_{SE1}, $SE1$ adds its identity, ID_{SE1}, nonce, N_{SE1}, and timestamp, T_{SE1}. These are included to ensure that the I-ICAAAN is fully achieved to secure the communication between $SE1$ and $SE2$. Here, the I-ICAAAN features include $CS(.)$, ID_{SE1}, $E(.), K_1$, K_2, $G_{SE1.SE2}$, N_{SE1} and T_{SE1}.

$$SE1 : E(M_{SE1}, ID_{SE1}, N_{SE1}, T_{SE1})_{K_1} \tag{1}$$

$$SE1 : G_{SE1.SE2} = CS(E(M_{SE1}, ID_{SE1}, N_{SE1}, T_{SE1})_{K_1}, K_2) \tag{2}$$

$$SE1 \rightarrow SE2 : [E(M_{SE1}, ID_{SE1}, N_{SE1}, T_{SE1})_{K_1} || G_{SE1.SE2}] \tag{3}$$

- Step 2: $SE2$ receives $E(M_{SE1}, ID_{SE1}, N_{SE1}, T_{SE1})_{K_1}$ and $G_{SE1.SE2}$, and runs $CV(.)$ on the $G_{SE1.SE2}$ to produce $G'_{SE1.SE2}$. If $G'_{SE1.SE2} = Yes$, $SE2$ accepts and decrypts the message.

$$SE2 : CV(G_{SE1.SE2}) = G'_{SE1.SE2} \tag{4}$$

$$G'_{SE1.SE2} = Yes \tag{5}$$

$$SE2 : D(M_{SE1}, ID_{SE1}, N_{SE1}, T_{SE1})_{K_1} \tag{6}$$

4.3. Intelligent Security System for Energy Management (ISSEM)

ISSEM is an intelligent security system that protects the EI against security vulnerabilities via computing relevant security metrics necessary for end-to-end security control thereby supporting energy management optimization. It can also be referred to as an Enterprise Resource Security Planning System. As IoT provides interoperability among different elements in EI, ISSEM uses IoT to leverage on Data Analytics System (DAS) to collect data [51] in the EI. The DAS examines the data collected from IoT and sends to the ISSEM's security components for security decision making. The security components include: 1) Business Intelligence Security (BIS) Component; 2) Artificial Intelligent Security (AIS) Component; and 3) Human-Computer Interaction Security (HCIS) Component. The interconnections among the security components are given in Figure 4. The brief descriptions and roles played by the security components are given below.

- Business Intelligence Security (BIS) Component: This is responsible for analysing and processing the data from DAS in order to identity and solve the security problems. This is considered as a basic level for security problem identification and resolution in EI. All the BIS solutions to the security problems identified have been configured in the ISSEM. Suppose a sensor in the EI is acting abnormally due to security causes, the BIS function is capable of identifying and solving the security problem, and returning the sensor to its default working state. All the BIS solutions to the security problems are based on I-ICAAAN in order to ensure effective security across the EI.

- Artificial Intelligence Security (AIS) Component: This is responsible for analysing the data from DAS in order to identity and learn to solve the security problems. This is an advanced level for solving security problems in EI. The AIS function has the ability to come up with

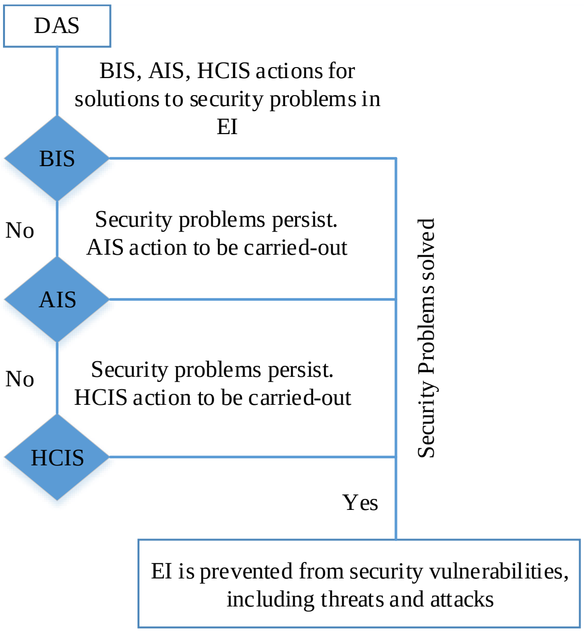

DAS
BIS, AIS, HCIS actions for solutions to security problems in EI
BIS
No
Security problems persist. AIS action to be carried-out
AIS
No
Security problems persist. HCIS action to be carried-out
HCIS
Security Problems solved
Yes
EI is prevented from security vulnerabilities, including threats and attacks

Figure 4: DAS and Security Components in ISSEM. Abbreviations: DAS - Data Analytics System, BIS - Business Intelligence Security, AIS - Artificial Intelligence Security, HCIS - Human-Computer Interaction Security.

solutions to the security problems, thus it doesnt reply on solutions configured in ISSEM. Based on the sensor that is acting abnormally, the AIS component is capable of learning and solving the problem, and returning the sensor to its previous normal working state. All the AIS solutions to the security problems are based on I-ICAAAN for adequate security in EI.

- Human-Computer Interaction Security (HCIS) Component: This is responsible for solving security problems with the help of human/operator. The data from DAS requires human input for security solution. Despite the help of human, all interactions are carried out actively and in a timely manner. To determine appropriate security solutions, an operator uses standard operating procedures during interaction, which is validated by the system for any human or unknown errors. To use the HCIS to solve the security problem associated with the abnormal behaviour of a sensor, the operator provides inputs to the system for security solution. Possible security problems requiring the HCIS in-

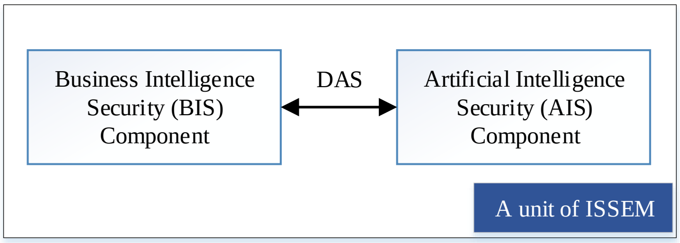

Business Intelligence Security (BIS) Component
DAS
Artificial Intelligence Security (AIS) Component
A unit of ISSEM

Figure 5: Intelligent Security Unit for Energy Management (ISUEM) in Energy Router. Abbreviations: DAS - Data Analytics System, ISSEM - Intelligent Security System for Energy Management.

clude social engineering and other security problems that occur across the IoT, ICT and cyber systems layer. All interactions between an operator and the system are based on I-ICAAAN.

An ISSEM unit that is presented as ISUEM is proposed for the energy router. A simple description of the ISUEM for the energy router is presented in Figure 5. The ISUEM is proposed to carry out BIS and AIS functionalities. For HCIS function, the energy router sends the data to the ISSEM via the DAS (based on I-ICAAAN). The ISUEM allows the energy router to communicate with the ISSEM. The ISSEM is the only system that is allowed to carry out HCIS function in order to ensure effective security monitoring and adequate security assurances of human inputs in EI. Thus, any HCIS function or unresolved security problem in the energy router is forwarded to the ISSEM for security solutions in a secure and timely fashion.

5. Evaluation

In this section, the evaluation of the proposed framework which attains high effectiveness in securing the EI is presented. We introduce an attack model to analyse the capabilities of the adversary in the EI. We analyse the security of I-ICAAAN, secure communication protocol and ISSEM followed by integrated privacy evaluation of the proposed framework.

5.1. Attack Model

We assume that the adversary is actively and passively monitoring the EI. The adversary can be internal or external. Once the EI is compromised, the adversary can intercept or falsify any messages. The Dolev-Yao Attack

Model [52] is followed which allows the adversary to accomplish the following goals: intercept, inject, replace, re-arrange, modify and collect messages in the EI. The Internal Adversary (IA) is a trusted user in the EI that has access to the EI and its resources, while the External Adversary (EA) is not a trusted user, but can carry out attacks from outside of the EI.

5.2. Security

In this subsection, we evaluate the proposed I-ICAAAN, secure communication protocol and ISSEM based on security in the EI.

5.2.1. I-ICAAAN Evaluation

The security of assets, data, network, users and software in the smart grid is required to prevent against security attacks. As much as security is a huge part of EI, we need to consider the system performance and complexity. Consider the case of an asset A, user U and MITM attacker M. Suppose that M wants to listen on the link between A and U. From the representation of the I-ICAAAN in EI, the identity of M cannot be verified in the EI and therefore access is denied. This implies that M will not be able to listen on the link. Thus, the system has detected a security attack, and further investigation is being carried out to prevent future security attacks.

5.2.2. Secure Communication Protocol Evaluation

We evaluate the secure communication protocol using the communication between $SE1$ and $SE2$. The proposed protocol is analysed from two aspects: 1) formal verification using AVISPA [53]; and 2) theoretical analysis to show its resilient against various security attacks.

1. Formal Verification: To evaluate the validity of the secure communication protocol, we use the AVISPA tool. AVISPA is a tool for analysing and verifying internet security protocols, and its one of the most trusted security tools for evaluating communication security. It uses back-end servers such as On-the-Fly Model-Checker (OFMC) [54] and Constraint-Logic-based Attack-Checker (Cl-AtSe) [55] to analyse the security of protocols and applications, taking into considerations various security attacks by adversaries. The simulation results are presented in the appendix, which show that the communication between $SE1$ and $SE2$ is secure and resilient against many security attacks.
2. Theoretical analysis showing resilient against various security attacks.

Proposition 2:. The proposed protocol is resilient against MITM attack, DoS attack, replay attack, impersonation attack, Sybil attack, false data injection attack and repudiation attack.

Proof:.

- Resilient against MITM attack: In the secure communication protocol, by verifying if $G'_{SE1.SE2} = Yes$, $SE2$ is checking the authenticity and integrity of the received message. Thus, this prevents MITM attack and an adversary cannot masquarade as a genuine component to carry out this attack.
- Resilient against DoS attack: In this attack, if $SE1$ knowingly or unknowingly enters incorrect ID_{SE1}, K_1, and K_2 to establish communication with $SE2$, the $CV(.)$ detects that the information used by $SE1$ are incorrect. Additonally, if an adversary enters incorrect ID and shared secret keys, $SE2$ detects the wrong information and avoids any data exchange with the adversary. Thus, the proposed protocol is safe from this attack.
- Resilient against replay attack: If an adversary intercepts and replaces M_{SE1}, $SE2$ verifies whether M_{SE1} is fresh using N_{SE1} and the event time using T_{SE1}. Thus, both N_{SE1} and T_{SE1} prevents this attack. Additionally, $CS(.)$ prevents the adversary from performing this attack. Therefore, these operations make our propotol secure against this attack.
- Resilient against impersonation attack: If an adversary successfully impersonates $SE1$, $SE2$ uses K_1, K_2 and ID_{SE1} to determine whether the adversary is legitimate. Since the adversay does not have K_1 and K_2, and cannot change ID_{SE1}, the adversary cannot impersonates $SE1$.
- Resilient against Sybil attack: In Sybil attack, the adversary falsifies the identity of many components. Since all components are identified and authenticated by the TA, the adversary is prevented from falsifying the identity of any genuine component. We assume that any component with multiple identities in EI will be automatically blacklisted by the TA.
- Resilient against false data injection attack: In this attack, through the combination of $CS(.)$, K_1, K_2 and $CV(.)$, the adversary is prevented from injecting false data into M_{SE1}. Additionally, N_{SE1}

Table 3: Comparison of Security Properties

Security Properties	**Schemes**			
	Minoli et al. [10]	**Yang et al. [11]**	**Elgargouri et al. [12]**	**Our Scheme**
Resilient against MITM attack	✓	−	✓	✓
Resilient against DoS attack	✓	−	✓	✓
Resilient against replay attack	✓	−	×	✓
Resilient against impersonation attack	✓	−	✓	✓
Resilient against Sybil attack	✓	−	✓	✓
Resilient against false data injection	×	✓	✓	✓
Resilient against repudiation attack	×	−	×	✓

− not applicable in the scheme.

and T_{SE1} support the prevention of this attack. Thus, our protocol is secure against this attack.

- Resilient against repudiation attack: In this attack, M_{SE1} from $SE1$ is tracked using $G_{SE1.SE2}$ with the support of utilising K_1 and K_2 as well as N_{SE1} and T_{SE1} for every communication. Thus, our protocol is safe from this attack.

Table 3 presents the comparison of security properties of our protocol and existing related schemes. We equipped the EI with security parameters capable of preventing many security attacks during communication. Referring to the TA as part of the energy domains that identifies and authenticates components before communication, it monitors and supports the protection of a component's identity in an offline mode. Furthermore, due to the non-existence of the TA during secure communication between components, our protocol prevents single point of failure and supports high availability of communication between components in the EI. Therefore, our protocol has the security characteristics for ensuring secure communication in EI.

5.2.3. ISSEM Evaluation

Here, we analyse the effectiveness of the ISSEM. Since the DAS acts as scheduler that selects and allocates security events/issues for best possible execution, a Nash-Equilibrium solution is applied to submit security issues to the BIS, AIS and HCIS functions for appropriate security actions. The ISSEM uses the proposed protocol to ensure end-to-end communication security amongst its security components and DAS. Due to the complexity of the EI environment, security functions are allocated by DAS based on Nash equilibrium solution of game theory. Generally, suppose in a standard game G=$(S_1, ..., S_n; f_1, ..., f_n)$ with n players, where S_i is the strategy set for player i, and f_i is its payoff function, the strategy profile $(S_1^*, S_2^*, ..., S_n^*)$ is a Nash Equilibrium if any player i selects S_i^* as the best strategy when other choose the strategy $(S_1^*, , S_{i-1}^* S_{i+1}^*, ..., S_n^*)$ with no derivations [56] [57] [58] [59]. In this paper, the standard game is presented by the DAS (represented as G) such that three-player game is modelled as a finite ordered element of three strategy profiles, together with a finite ordered of three playoffs. Suppose each player i in 1,2 and 3 has chosen a strategy S_i. This yields the strategy profile $S = (S_1^*, S_2^*, S_3^*)$, in which player i will get in return payoff $f_i(S)$. The strategy profile (S_1^*, S_2^*, S_3^*) is a Nash equilibrium if any single player i selects S_i^* as the best strategy when other choose the strategy (S_1^*, S_{i-1}^*) with no deviations. In this case, if HCIS is assigned to carry-out HCIS function, both BIS and AIS cannot carry-out such function irrespective of any form of abnormalities.

Now, we consider possible targets on the BIS, AIS and HCIS by an attacker. The DAS represents the defender capable of taking the defense actions. We define set of desired concurrent attack and defense actions by attacker, A, and defender, D, respectively as follows:

$$A = t_1^a, t_2^a, t_3^a \tag{7}$$

$$D = t_1^d, t_2^d, t_3^d \tag{8}$$

where A represent the attack actions and D represent the defense actions. All actions undertaken by each player cannot exceed the total number of resources available, i.e.

$$C_n^A = \sum_{i \in t_n^a} C_i^a \leqslant R_A \tag{9}$$

$$C_n^D = \sum_{i \in t_n^d} C_i^d \leqslant R_D \tag{10}$$

where C_n^A is the cost of the attacker implementing attack action t_n^a, C_n^D is the cost of the defender for implementing the defense action t_n^d. C_i^a is the cost of attacking the component i, C_i^d is the cost of defending the component i. Since all communications in EI are I-ICAAAN based, we also define set of desired I-ICAAAN action by the TA in EI.

$$IC_n^{ta} = IC_1^{ta}, IC_2^{ta}, IC_3^{ta} \tag{11}$$

where IC_n^{ta} represent the TA actions to ensure I-ICAAAN based communication across the ISSEM. The total cost of actions undertaken by the TA is given by:

$$C_n^{TA} = \sum_{i \in ic_n^{ta}} C_i^{ta} \leqslant R_{TA} \tag{12}$$

where C_n^{TA} is the cost of the TA for implementing the I-ICAAAN action ic_n^{ta} and C_i^{ta} is the cost of ensuring that all communications are based on I-ICAAAN.

The Playoff of the players are given by:

$$f_A = C_D - C_A * C_{TA} \tag{13}$$

$$f_D = C_A - C_D * C_{TA} \tag{14}$$

where f_A is the playoff of the attacker, f_D is the playoff of the defender, C_D is the cost of the defender to perform a defense action, C_A is the cost of the attacker to perform an attack action, C_{TA} is the cost of the trusted authority to ensure I-ICAAAN. Since the attacker cannot determine C_{TA}, this shows that the attacker cannot computef_A, thus no value is received by the attacker at the end of the game. This shows that our I-ICAAAN has provided security to the ISSEM and its security components.

5.3. Privacy

We evaluate the proposed framework based on privacy by integrating the I-ICAAAN, secure communication protocol and ISSEM. In EI, privacy is ensured across the components, data and events. EI will not allow the use of data or any resources until the I-ICAAAN has been confirmed thereby assisting to prevent against privacy attack. An attacker could be located inside or outside the EI architecture in order to steal or reveal information about any components or events. An EA will not be able identify a specific component's information because all components use different identities and attributes to request or exchange any data. An IA could be one of the energy domain entities that knows about the basic configuration of the EI. IA needs to be identified and authenticated by the TA and all components are assigned nonrepudiation security parameter. Since the I-ICAAAN of the attackers, EA and IA, cannot be verified, information or events cannot be shared with the attackers thereby maintaining privacy. In addition, data confidentiality and integrity in EI can be achieved via privacy. Therefore, the I-ICAAAN has also been used to achieve privacy via automatically not disclosing any information to the attackers. The cyber security policy in LSA is also used to communicate and enforce privacy in an automated fashion. The I-ICAAAN provides additional level of privacy to components, data and events in EI when compared to the smart grid privacy features. Furthermore, we also use the I-ICAAAN to add privacy and confidentiality to components, data and events in order to maintain components and events integrity.

6. Conclusion and Future Works

We have proposed a cyber security framework for IoT-based Energy Internet, which comprises of an identity-based security mechanism (I-ICAAAN), a secure communication protocol and an Intelligent Security System for Energy Management (ISSEM). The framework provides adequate security and privacy to components, data and events, and supports enhanced energy management in the Energy Internet. Using AVISPA tool and theoretical analysis, we showed that the secure communication protocol is resilient against many security attacks and it is superior to existing related schemes. The correctness of the ISSEM is confirmed by the proof with Nash Equilibrum. The evaluation results show that our proposed framework is secure and efficient for the Energy Internet. As part of our ongoing work, we plan to develop secure and lightweight key exchange schemes for secure unicast, multicast and broadcast communications in the Energy Internet.

References

[1] Shapsough, S., Qatan, F., Aburukba, R., Aloul, F. and Al Ali, A.R., 2015, October. Smart Grid cyber security: Challenges and solutions. In Smart Grid and Clean Energy Technologies (ICSGCE), 2015 International Conference on (pp. 170-175). IEEE.

[2] Zhou, X., Wang, F. and Ma, Y., 2015, August. An overview on energy internet. In Mechatronics and Automation (ICMA), 2015 IEEE International Conference on (pp. 126-131). IEEE.

[3] Cao, J. and Yang, M., 2013, December. Energy internet–towards smart grid 2.0. In Networking and Distributed Computing (ICNDC), 2013 Fourth International Conference on (pp. 105-110). IEEE.

[4] Rifkin, J., 2011. The third industrial revolution. New York, 291.

[5] Ejaz, W., Naeem, M., Shahid, A., Anpalagan, A. and Jo, M., 2017. Efficient energy management for the internet of things in smart cities. IEEE Communications Magazine, 55(1), pp.84-91.

[6] Collier, S.E., 2015, April. The emerging enernet: Convergence of the smart grid with the internet of things. In Rural Electric Power Conference (REPC), 2015 IEEE (pp. 65-68). IEEE.

[7] Xu, Y., Zhang, J., Wang, W., Juneja, A. and Bhattacharya, S., 2011, October. Energy router: Architectures and functionalities toward Energy Internet. In Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on (pp. 31-36). IEEE.

[8] Bui, N., Castellani, A.P., Casari, P. and Zorzi, M., 2012. The internet of energy: a web-enabled smart grid system. IEEE Network, 26(4).

[9] Huang, A.Q., Crow, M.L., Heydt, G.T., Zheng, J.P. and Dale, S.J., 2011. The future renewable electric energy delivery and management (FREEDM) system: the energy internet. Proceedings of the IEEE, 99(1), pp.133-148.

[10] Minoli, D., Sohraby, K. and Occhiogrosso, B., 2017. IoT Considerations, Requirements, and Architectures for Smart BuildingsEnergy Optimization and Next-Generation Building Management Systems. IEEE Internet of Things Journal, 4(1), pp.269-283.

[11] Yang, X., Zhao, P., Zhang, X., Lin, J. and Yu, W., 2017. Toward a Gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid. IEEE Internet of Things Journal, 4(1), pp.147-161.

[12] Elgargouri, A., Virrankoski, R. and Elmusrati, M., 2015, March. IEC 61850 based smart grid security. In Industrial Technology (ICIT), 2015 IEEE International Conference on (pp. 2461-2465). IEEE.

[13] Yu, X. and Xue, Y., 2016. Smart grids: A cyberphysical systems perspective. Proceedings of the IEEE, 104(5), pp.1058-1070.

[14] Yan, J., He, H., Zhong, X. and Tang, Y., 2017. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. IEEE Transactions on Information Forensics and Security, 12(1), pp.200-210.

[15] Hu, J. and Vasilakos, A.V., 2016. Energy big data analytics and security: challenges and opportunities. IEEE Transactions on Smart Grid, 7(5), pp.2423-2436.

[16] Hu, B. and Gharavi, H., 2014. Smart grid mesh network security using dynamic key distribution with merkle tree 4-way handshaking. IEEE Transactions on Smart Grid, 5(2), pp.550-558.

[17] Saxena, N., Choi, B.J. and Lu, R., 2016. Authentication and authorization scheme for various user roles and devices in smart grid. IEEE Transactions on Information Forensics and Security, 11(5), pp.907-921.

[18] Badra, M. and Zeadally, S., 2014. Design and performance analysis of a virtual ring architecture for smart grid privacy. IEEE transactions on information forensics and security, 9(2), pp.321-329.

[19] Liu, S., Liu, X.P. and El Saddik, A., 2013, February. Denial-of-Service (DoS) attacks on load frequency control in smart grids. In Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES (pp. 1-6). IEEE.

[20] Kosut, O., Jia, L., Thomas, R.J. and Tong, L., 2011. Malicious data attacks on the smart grid. IEEE Transactions on Smart Grid, 2(4), pp.645-658.

[21] Liu, R., Vellaithurai, C., Biswas, S.S., Gamage, T.T. and Srivastava, A.K., 2015. Analyzing the cyber-physical impact of cyber events on the power grid. IEEE Transactions on Smart Grid, 6(5), pp.2444-2453.

[22] Esmalifalak, M., Shi, G., Han, Z. and Song, L., 2013. Bad data injection attack and defense in electricity market using game theory study. IEEE Transactions on Smart Grid, 4(1), pp.160-169.

[23] Chen, T.M., Sanchez-Aarnoutse, J.C. and Buford, J., 2011. Petri net modeling of cyber-physical attacks on smart grid. IEEE Transactions on Smart Grid, 2(4), pp.741-749.

[24] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P. and Poolla, K., 2013. Smart grid data integrity attacks. IEEE Transactions on Smart Grid, 4(3), pp.1244-1253.

[25] Sridhar, S., Hahn, A. and Govindarasu, M., 2012. Cyberphysical system security for the electric power grid. Proceedings of the IEEE, 100(1), pp.210-224.

[26] Wang, K., Yu, J., Yu, Y., Qian, Y., Zeng, D., Guo, S., Xiang, Y. and Wu, J., 2017. A survey on energy internet: Architecture, approach, and emerging technologies. IEEE Systems Journal.

[27] Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X., 2017. Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, 21(2), pp.34-42.

[28] Sajid, A., Abbas, H. and Saleem, K., 2016. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access, 4, pp.1375-1384.

[29] Ghosh, D., Ghose, T. and Mohanta, D.K., 2013. Communication feasibility analysis for smart grid with phasor measurement units. IEEE Transactions on Industrial Informatics, 9(3), pp.1486-1496.

[30] Srinivasan, D. and Reindl, T., 2015, November. GIS as a tool for enhancing the optimization of demand side management in residential microgrid. In Innovative Smart Grid Technologies-Asia (ISGT ASIA), 2015 IEEE (pp. 1-6). IEEE.

[31] Srinivasan, D. and Reindl, T., 2015, November. Real-time display of data from a smart-grid on geographical map using a GIS tool and its role in optimization of game theory. In Innovative Smart Grid Technologies-Asia (ISGT ASIA), 2015 IEEE (pp. 1-6). IEEE.

[32] Zhu, C., Leung, V.C., Shu, L. and Ngai, E.C.H., 2015. Green Internet of Things for smart world. IEEE Access, 3, pp.2151-2162.

[33] Sathyamoorthy, P., Ngai, E.C.H., Hu, X. and Leung, V.C., 2015, November. Energy efficiency as an orchestration service for mobile Internet of Things. In Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on (pp. 155-162). IEEE.

[34] Poslad, S., Middleton, S.E., Chaves, F., Tao, R., Necmioglu, O. and Bgel, U., 2015. A semantic IoT early warning system for natural environment crisis management. IEEE Transactions on Emerging Topics in Computing, 3(2), pp.246-257.

[35] Pillitteri, V.Y. and Brewer, T.L., 2014. Guidelines for smart grid cybersecurity. NIST Interagency/Internal Report (NISTIR)-7628 Rev 1.

[36] Lin, C.C., Deng, D.J., Liu, W.Y. and Chen, L., 2017. Peak Load Shifting in the Internet of Energy With Energy Trading Among End-Users. IEEE Access, 5, pp.1967-1976.

[37] Boyes, H., 2015. Security, Privacy, and the Built Environment. IT Professional, 17(3), pp.25-31.

[38] Barki, A., Bouabdallah, A., Gharout, S. and Traor, J., 2016. M2M security: Challenges and solutions. IEEE Communications Surveys and Tutorials, 18(2), pp.1241-1254.

[39] La, Q.D., Quek, T.Q., Lee, J., Jin, S. and Zhu, H., 2016. Deceptive attack and defense game in honeypot-enabled networks for the internet of things. IEEE Internet of Things Journal, 3(6), pp.1025-1035.

[40] Tamani, N. and Ghamri-Doudane, Y., 2016, July. Towards a user privacy preservation system for IoT environments: a habit-based approach. In Fuzzy Systems (FUZZ-IEEE), 2016 IEEE International Conference on (pp. 2425-2432). IEEE.

[41] Bellagente, P., Ferrari, P., Flammini, A., Rinaldi, S. and Sisinni, E., 2016, May. Enabling PROFINET devices to work in IoT: Characterization and requirements. In Instrumentation and Measurement Technology Conference Proceedings (I2MTC), 2016 IEEE International (pp. 1-6). IEEE.

[42] Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S. and Sheng, Q.Z., 2017. IoT middleware: A survey on issues and enabling technologies. IEEE Internet of Things Journal, 4(1), pp.1-20.

[43] Park, C.S., 2017. A Secure and Efficient ECQV Implicit Certificate Issuance Protocol for the Internet of Things Applications. IEEE Sensors Journal, 17(7), pp.2215-2223.

[44] Al Faruque, M.A. and Vatanparvar, K., 2016. Energy management-as-a-service over fog computing platform. IEEE internet of things journal, 3(2), pp.161-169.

[45] Annex, V., 2012. Smart grid security.

[46] Gessner, D., Olivereau, A., Segura, A.S. and Serbanati, A., 2012, June. Trustworthy infrastructure services for a secure and privacy-respecting internet of things. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 998-1003). IEEE.

[47] Ning, H., Liu, H. and Yang, L.T., 2013. Cyberentity security in the internet of things. Computer, 46(4), pp.46-53.

[48] Liu, J. and Sun, W., 2016. Smart Attacks against Intelligent Wearables in People-Centric Internet of Things. IEEE Communications Magazine, 54(12), pp.44-49.

[49] Zhang, Z.K., Cho, M.C.Y., Wu, Z.Y. and Shieh, S.W., 2015. Identifying and Authenticating IoT Objects in a Natural Context. Computer, 48(8), pp.81-83.

[50] Dworkin, M.J., 2016. Recommendation for block cipher modes of operation: The CMAC mode for authentication. Special Publication (NIST SP)-800-38B.

[51] Ahlgren, B., Hidell, M. and Ngai, E.C.H., 2016. Internet of Things for Smart Cities: Interoperability and Open Data. IEEE Internet Computing, 20(6), pp.52-56.

[52] Dolev, D. and Yao, A., 1983. On the security of public key protocols. IEEE Transactions on information theory, 29(2), pp.198-208.

[53] Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cullar, J., Drielsma, P.H., Ham, P.C., Kouchnarenko, O., Mantovani, J. and Mdersheim, S., 2005, July. The AVISPA tool for the automated validation of internet security protocols and applications. In International conference on computer aided verification (pp. 281-285). Springer, Berlin, Heidelberg.

[54] Basin, D., Mdersheim, S. and Vigano, L., 2005. OFMC: A symbolic model checker for security protocols. International Journal of Information Security, 4(3), pp.181-208.

[55] Turuani, M., 2006, August. The CL-Atse protocol analyser. In International Conference on Rewriting Techniques and Applications (pp. 277-286). Springer, Berlin, Heidelberg.

[56] Zhou, Z., Xiong, F., Huang, B., Xu, C., Jiao, R., Liao, B., Yin, Z. and Li, J., 2017. Game-Theoretical Energy Management for Energy Internet With Big Data-Based Renewable Power Forecasting. IEEE Access, 5, pp.5731-5746.

[57] Sanjab, A. and Saad, W., 2016. Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective. IEEE Transactions on Smart Grid, 7(4), pp.2038-2049.

[58] Spata, M.O., 2007, June. A Nash-Equilibrium Based Algorithm for Scheduling Jobs on a Grid Cluster. In Enabling Technologies: Infrastructure for Collaborative Enterprises, 2007. WETICE 2007. 16th IEEE International Workshops on (pp. 251-252). IEEE.

[59] Esnaola, I., Perlaza, S.M., Poor, H.V. and Kosut, O., 2016. Maximum distortion attacks in electricity grids. IEEE Transactions on Smart Grid, 7(4), pp.2007-2015.

Appendix

Table : Analysis Output from OFMC and CL-Atse Backends in AVISPA

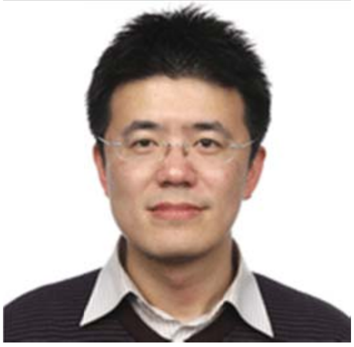
OFMC Backend	CL-Atse Backend
% OFMC	SUMMARY
% Version of 2006/02/13	SAFE
SUMMARY	DETAILS
SAFE	BOUNDED_NUMBER_OF_
DETAILS	SESSIONS
BOUNDED_NUMBER_OF_SESSIONS	TYPED_MODEL
PROTOCOL	PROTOCOL
/home/span/span/testsuite/results/CSF.if	/home/span/span/testsuite/
GOAL	results/CSF.if
as_specified	GOAL
BACKEND	As Specified
OFMC	BACKEND
COMMENTS	CL-AtSe
STATISTICS	STATISTICS
parseTime: 0.00s	Analysed: 0 states
searchTime: 0.02s	Reachable: 0 states
visitedNodes: 3	Translation: 0.00 seconds
depth: 6 piles	Computation: 0.00 seconds

The simulation results presented in the table above represent the following: 1) our proposed protocol is safe from Dolev-Yao attack model; 2) the OFMC and CL-AtSe Backends reported that the proposed protocol is safe; 3) DETAILS indicated that the conditions of all sessions of the proposed protocol are safe. Hence, the proposed scheme is safe and resilience against various security attacks.

Author Biography

Author Name	Author Biography
Abubakar Sadiq Sani	**Abubakar Sadiq Sani** received MSc. Degree in Computer and Network Security from Middlesex University, London, United Kingdom, in 2012, and the Professional Education in Applied Cyber Security from Massachusetts Institute of Technology, Cambridge, United States of America, in 2014. He is a Certified Ethical Hacker and EC-Council Security Analyst. He worked in the industry for a few years until he joined The University of Sydney as a Ph.D. candidate. He is currently working towards a Ph.D. degree at the School of Electrical and Information Engineering, The University of Sydney, Australia. His primary research interests include cyber security for energy internet and smart grid applications, physical layer security for communication networks, scheduling and network coding for cyber physical systems, and integration of enterprise resource planning, internet of things and cloud computing.
Dong Yuan	**Dong Yuan** received the Ph.D. degree from Swinburne University of Technology, Australia, in 2012. He is a lecturer in School of Electrical and Information Engineering, The University of Sydney, Australia. His research interests include cloud computing, data management in parallel and distributed systems, scheduling and resource management, business process management and workflow systems.
Jiong Jin	**Jiong Jin** received the Ph.D. degree from the Department of Electrical and Electronic Engineering, The University of Melbourne, Parkville, Australia, in 2011. He is currently a Lecturer in robotics and mechatronics as a member of the Faculty of Science, Engineering and Technology, Swinburne University of Technology, Melbourne, Australia. From 2011 to 2013, he was a Research Fellow with The University of Melbourne. His research interests include network optimization, nonlinear systems and sliding mode control, robotics, wireless sensor networks, Internet of Things and Future Internet, cyber-physical systems, and applications in smart grids and smart cities.
Longxiang Gao	**Longxiang Gao** received his Ph.D. in Computer Science from Deakin University, Australia. He is currently a Lecturer at School of Information Technology, Deakin University to teach database, web development and networking units for both undergraduate and postgraduate students. Before joined Deakin University, he was a post-doctoral research fellow at IBM Research & Development Australia. In IBM R&D, he had been the core team member to develop a crisis event analysis, computing and reporting system to Australia Red Cross, and this project has been selected as the feature project of IBM. His research interests include data processing, mobile social networks, Fog computing and network security
Shui Yu	**Shui Yu** received the Ph.D. (Computer Science) from Deakin University in 2004. He is currently a Senior Lecturer of School of Information Technology, Deakin University, Melbourne, Australia. Before joining Deakin University, Dr Yu was a Lecturer of Computer College in University of Electronic Science and Technology of China. He has a good experience of industry, especially in network design and software development organization and implementation. His research interests include networking theory and network security, especially security, privacy and information forensics on the Internet. He targets on narrowing the gap between theory and applications using mathematical tools.
Zhao Yang Dong	Professor Z.Y. (Joe) Dong received the Ph.D. degree from the University of Sydney, Australia, in 1999. He is Head of School of Electrical and Information Engineering, the University of Sydney, and a contractor with Ausgrid and EPRI, USA. He is now a member of the ARC College of Experts. Prior to joining the University of Sydney in 2013, he was Ausgrid Chair and Director of Ausgrid Centre of Excellence for Intelligent Electricity Networks (CIEN) at the University of Newcastle, Australia. He has also worked for Hong Kong Polytechnic University and as system planning manager with Transend Networks, Australia. Professor Dong's research interest includes power system planning and stability, smart grid, load modeling, renewable energy, electricity market, and computational methods. He is an editor of IEEE TRANSACTIONS ON SMART GRID, IEEE PES LETTERS, IET RENEWABLE POWER GENERATION, and Journal of Modern Power Systems and Clean Energy. He is an international Advisor for the lead Chinese journal of Automation of Electric Power Systems. He also serves as guest editor for International Journal of Systems Science.

Author Photo

Author Name	Author Photo
Abubakar Sadiq Sani	
Dong Yuan	
Jiong Jin	
Longxiang Gao	

Shui Yu	
Zhao Yang Dong	

Cyber Security Framework for Internet of Things-Based Energy Internet

Highlights

- The security and privacy of components, data and events in the Energy Internet.
- The framework relies on an identity-based security mechanism.
- A secure communication protocol that provides secure data exchange.
- An Intelligent Security System for Energy Management to handle security metrics.
- The framework prevents security attacks and support energy management.