The Essential Identified Consumer Requirements Derived through Descriptive Analysis On the Information Security in a Smart Grid System

Amy Poh Ai Ling[1], Chen Yan Yu[1], Sugihara Kokichi[1], Mukaidono Masao[2]

[1]Department of Mathematical Modeling Analysis, and Simulation, Graduate School of Advanced Mathematical Sciences, Meiji University, Kanagawa, Japan.

[2]Computer Science Department, School of Science and Technology, Meiji University, Kanagawa, Japan.

Abstract: *The purpose of this paper was to measure the essentiality of the identified consumer requirements on the information security in a smart grid system, focuses mainly on helping government and utilities providers, when enhancing their system processes, to develop and prioritize the necessary requirements for securing their information in a smart grid. This paper examined on the voice of customer perceived by the respondents towards smart grid. The major finding of this paper exhibits the agreement from the respondent on the essentiality of the identified sixteen consumer requirements and the correlation between each requirement. The result of the ranking was a mixture of from five categories of philosophy, human behavior, rule based social system, strategic system and hardware, and hence each category could be concluded to have a balance value of essentiality. Chi-Square test proved that all variables are significant. Individual value plot versus country shows that the rapidly growing economies in different countries have different smart grid infrastructure needs. Pearson correlation test showed that security in wireless media has very low correlation with others variable as it is still in its development process. Lexicographical order test showed that integrity, quality assurance and high bandwidth of communications channels has high correlation with each other. Correlation relationship ring, cluster and tree concluded that the items in the hardware category are highly correlated to each other. The success of this effort appeared to hinge on utility companies championing information system security initiatives and propagating an awareness of the importance of information security among consumers at all levels of the community.*

Keywords: *smart grid, information security, consumer requirement, descriptive analysis, Pearson correlation, correlation relationship ring.*

I. INTRODUCTION

One reason for putting a magnifier over the security term in an information pool of the smart grid system was that cyber technology depends much on its control management to create certain assurance on its protected information stored. Another reason, perhaps more important than the first, was that the security allows the consumer to gain trust towards the service they utilized. For example, many people surfing the net to find out what information will be uploaded to the grid once they become a smart grid user. Others may concern only the benefit a smart grid system brings. Those wanting to go deeper may look at the entire system, its contribution towards environment, cost saving feasibility, and so on. Smart grid has been recognizes as a growing potential and sustainable solution for energy issue. A system will grow strong when it continuously gained its consumer trust and support, thus consumer is one of the key element. In order to realize the smart grid, data were gathered from large numbers of intelligent sensors and processors installed on the power lines and equipment on the distribution grid. This data collected will be transferred to central information processing systems, which both present the information to operators and use the information to send back control settings. While information and communication seems to be much more important compare to decades ago, the system has to be incredibly strong to protect itself against hackers' attacks. The objective of this study was to measure the essentiality of information security requirement based on the consumer perceived significance and the correlation between each requirement.

II. Literature Review

2.1 Technological transfer phenomenon – Grid technology

Modeling lifestyle effects on energy demand, the increase of societal energy consumption was influenced by three main items: technical efficiency, lifestyles and socio-cultural factors. Technological transfer phenomenon was often seen as a crucial part that contributes to the solutions of environmental highlights. However, when technological change was seen from the perspective of everyday life, this image becomes more complex [1, 2]. Grid technology provides the chance for a simple and transparent access to different information sources. This idea was proven when the data grid can be interpreted as the consolidation of different data managing systems furnishing the user with data, information and knowledge [3]. With the changes of smart grid and other in the electricity utility industries, new demands on the telecom networks were generated [4].

2.2 Consumer's impact towards the information security system

When the information was shared real-time between power generators, distributed resources, service provider, control center, substation, and even to end-users, any changes exposed to a hacker's attack would bring the whole system down into a mess. This will dangerously create consumer distrust and dissatisfaction that may lead to other more destructive phenomenon.

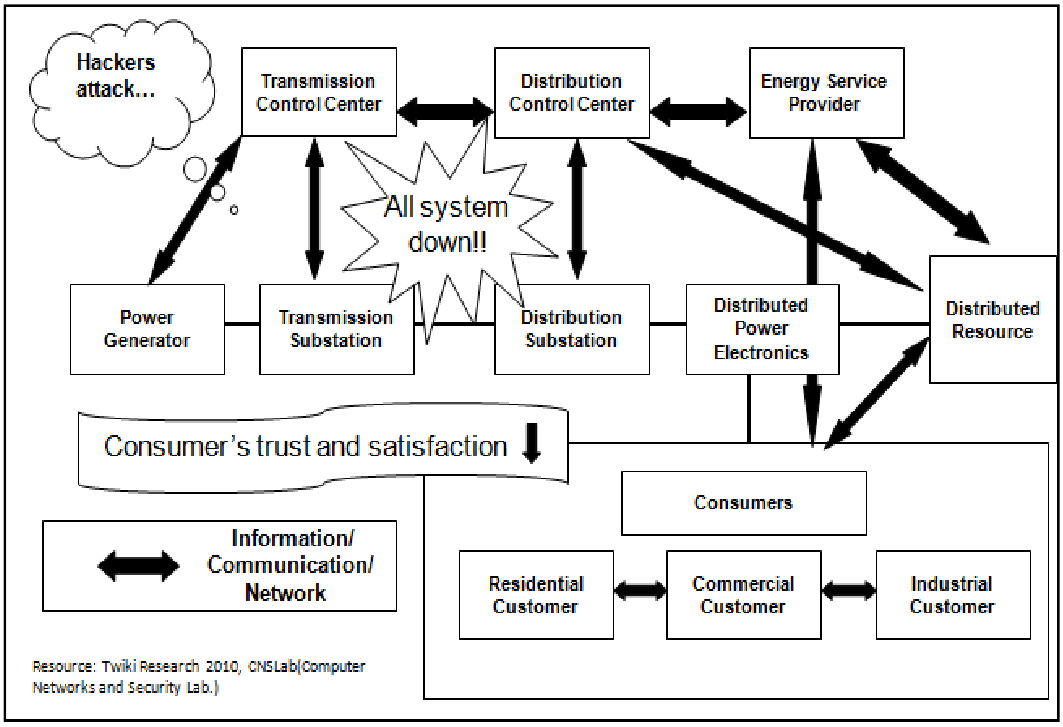

Hackers attack…
Transmission Control Center
Distribution Control Center
Energy Service Provider
All system down!!
Power Generator
Transmission Substation
Distribution Substation
Distributed Power Electronics
Distributed Resource
Consumer's trust and satisfaction
Information/ Communication/ Network
Consumers
Residential Customer
Commercial Customer
Industrial Customer
Resource: Twiki Research 2010, CNSLab(Computer Networks and Security Lab.)

Figure. 1. Security Importance [5].

As the consumer's awareness and participation in the smart grid project has increased, it is interesting to note what criteria held by the consumer will impact the information security system. The importance of information security criteria was the main aspect perceived to impact customer trust towards the entire smart grid system [6], as shown in figure 1.

2.3 Smart Grid Conceptual Mind Mapping

Figure 2 below showed Smart grid conceptual mapping where the study area was highlighted. Under the umbrella of Smart Planet cultivated by IBM, lay Smart Water Management and Green Planet, Smarter Planet Skill and Education, Smart Grid, Smart Health Care and Smart Cities. There were eight main elements in Smart Grid, narrowing down to network security utilities, business network, communication and information security's impact on consumer trust and satisfaction which was the main focus of this paper. Smart grid utilizes communication technology and information to optimally transmit and distribute electricity from suppliers to consumers.

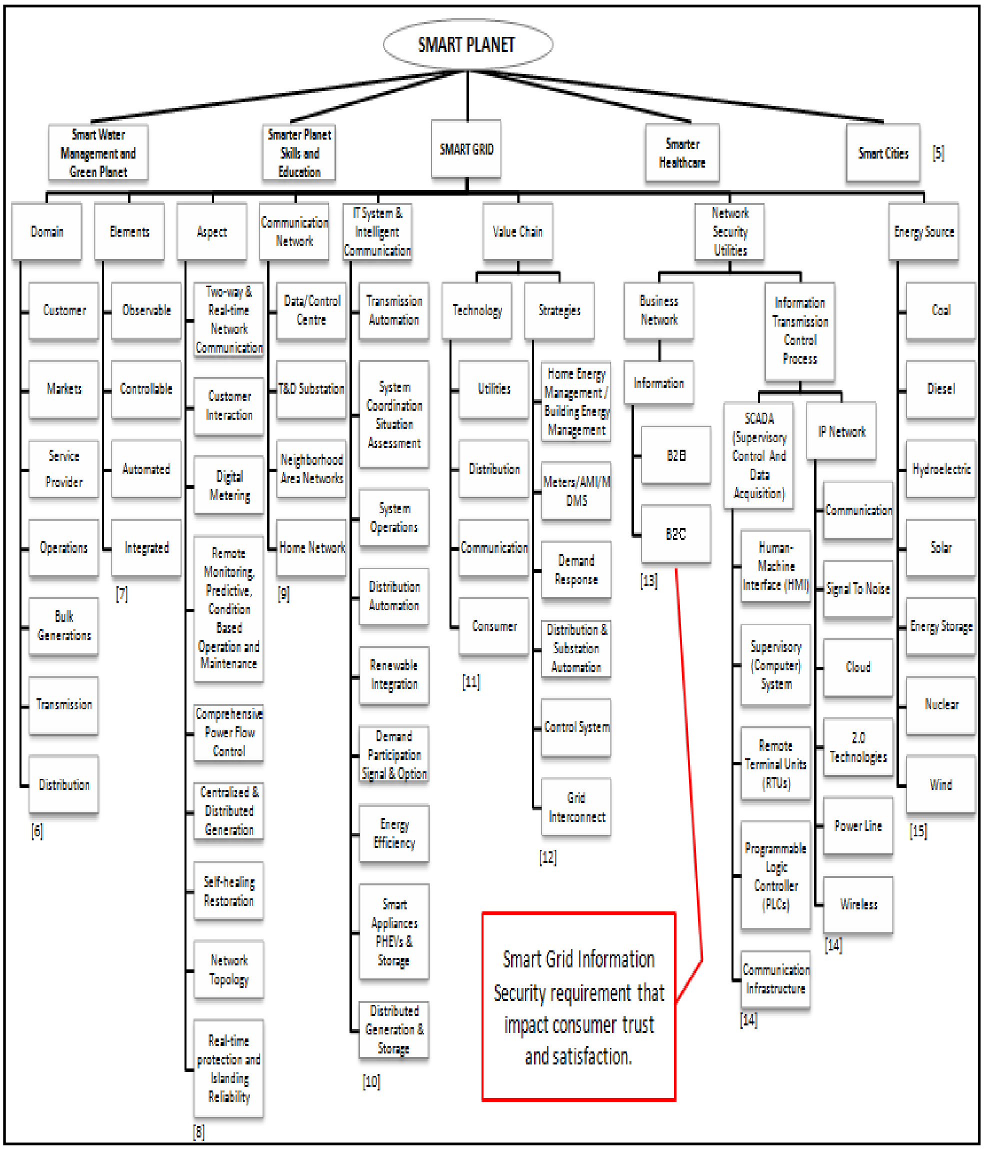

SMART PLANET
Smart Water Management and Green Planet
Smarter Planet Skills and Education
SMART GRID
Smarter Healthcare
Smart Cities
[5]
Domain
Elements
Aspect
Communication Network
IT System & Intelligent Communication
Value Chain
Network Security Utilities
Energy Source
Customer
Markets
Service Provider
Operations
Bulk Generations
Transmission
Distribution
[6]
Observable
Controllable
Automated
Integrated
[7]
Two-way & Real-time Network Communication
Customer Interaction
Digital Metering
Remote Monitoring, Predictive, Condition Based Operation and Maintenance
Comprehensive Power Flow Control
Centralized & Distributed Generation
Self-healing Restoration
Network Topology
Real-time protection and Islanding Reliability
[8]
Data/Control Centre
T&D Substation
Neighborhood Area Networks
Home Network
[9]
Transmission Automation
System Coordination Situation Assessment
System Operations
Distribution Automation
Renewable Integration
Demand Participation Signal & Option
Energy Efficiency
Smart Appliances PHEVs & Storage
Distributed Generation & Storage
[10]
Technology
Utilities
Distribution
Communication
Consumer
[11]
Strategies
Home Energy Management / Building Energy Management
Meters/AMI/M DMS
Demand Response
Distribution & Substation Automation
Control System
Grid Interconnect
[12]
Business Network
Information
B2B
B2C
[13]
Information Transmission Control Process
SCADA (Supervisory Control And Data Acquisition)
Human-Machine Interface (HMI)
Supervisory (Computer) System
Remote Terminal Units (RTUs)
Programmable Logic Controller (PLCs)
Communication Infrastructure
[14]
IP Network
Communication
Signal To Noise
Cloud
2.0 Technologies
Power Line
Wireless
[14]
Coal
Diesel
Hydroelectric
Solar
Energy Storage
Nuclear
Wind
[15]
Smart Grid Information Security requirement that impact consumer trust and satisfaction.

Figure. 2. Smart Grid Conceptual Mind Mapping [6].

2.4 The need to protect the privacy and security of priceless data

Personal information leakage incidents could be vital and cost a big sum of compensation to the utilities. The number of victims of information leakage incidents for 2008 amounted to 7.23 million individuals, the following table 1 shows the summary of data collected for 2008 in the Information Security Incident Survey Report of NPO Japan Network Security Association Security Incident Investigation Working Group.

Table 1. Summary Data of 2008 Personal Information Leakage Incidents [7]

Number of Victims	7,232,763
Number of Incidents	1,373
Total Projected Compensation for Damages	¥236,725,290,000
Number of Victims per Incident *1	5,668
Average Projected Compensation for Damages per Incident *1	¥185,520,000
Average Projected Compensation for Damages per Victim *2	¥43,632

A number of smart grid information security requirements and regulations were available online, those guidelines were a significant step in securing the smart grid but they do not fully address potential vulnerabilities that can emerge [8, 9]. The strongest arguments made for securing smart meters, saying that consumers will have physical and potentially logical access to the smart meters [10]. Security was generally described in terms of availability, integrity, and confidentiality. Cyber systems were observed to be vulnerable to worms, viruses, denial-of-service attacks, malware, phishing, and user errors that compromise integrity and availability [11].

It is important to avoid baring any potential security risk. As a matter of fact, grid security technologies have been so far designed and deployed as a middleware layer add-on, independently at each tier [12]. The need to protect the privacy and security of priceless data over the grid was fueling even more need for common security evaluation criteria. In brief, information security professionals need to be aware that the workings of the most basic IT resource of electricity supply is changing in a manner that introduces a far larger and remotely addressable attack surface combined with the tempting opportunity for mischief and monetary gain [13].

III. 3 SIGNIFICANCE OF THE STUDY

Because a smart grid utilizes digital technology to provide two-way communication between suppliers and consumers home electronics through the use of smart meters, information security protection measures need to be consumer friendly and practicable to be implemented on all level within a community or organization [14]. For this reason, it is important for us to examine on the voice of customer on their agreement on the essentiality of the identified sixteen consumer requirements [6], and the ranking of essentiality of the requirements. The correlation relationship between the requirements will show how a trend will change when a requirement is being implemented or abolished, aim is to provide a deeper investigation into the information cues on security requirements that really attract consumer interest and therefore may merit specific attention in future information security policies.

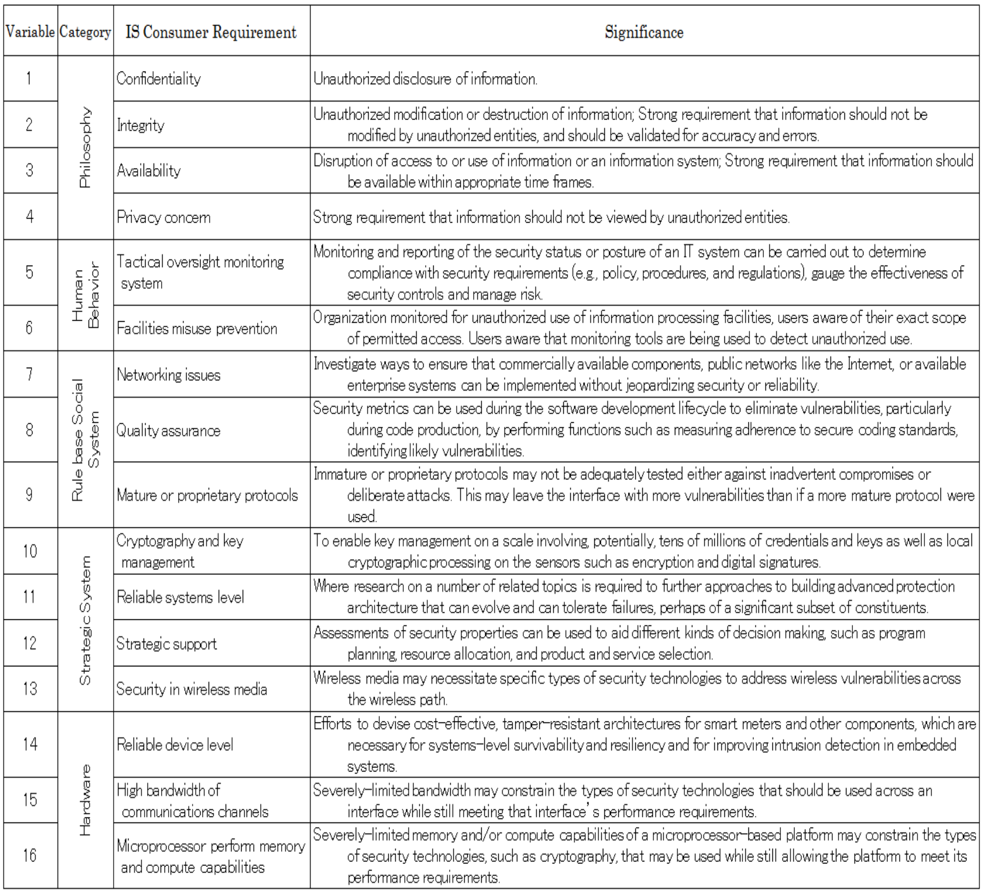
IV. METHODOLOGY

4.1 Hermeneutic Circle: Consumer Requirements Identified

Hermeneutic Circle is an interpretive and conceptual-analytical research method. Hermeneutics refers to the idea that one understands of the text as a whole is established by reference to the individual parts and one understands of each individual part in reference to the whole [15, 16, 17]. The information security consumer requirements were carefully picked from literature review, referring to experts' opinions and focused group discussion.

Table 2 referred to the sixteen requirements that were identified via the work of voice of customer and careful literature review based on Hermeneutic Circle Methodology classed in five categories of philosophy, human behavior, rule based social system, strategic system and hardware.

Table 2. Information Security Consumer Requirements and its Significant



Variable	Category	IS Consumer Requirement	Significance
1	Philosophy	Confidentiality	Unauthorized disclosure of information.
2		Integrity	Unauthorized modification or destruction of information; Strong requirement that information should not be modified by unauthorized entities, and should be validated for accuracy and errors.
3		Availability	Disruption of access to or use of information or an information system; Strong requirement that information should be available within appropriate time frames.
4		Privacy concem	Strong requirement that information should not be viewed by unauthorized entities.
5	Human Behavior	Tactical oversight monitoring system	Monitoring and reporting of the security status or posture of an IT system can be carried out to determine compliance with security requirements (e.g., policy, procedures, and regulations), gauge the effectiveness of security controls and manage risk.
6		Facilities misuse prevention	Organization monitored for unauthorized use of information processing facilities, users aware of their exact scope of permitted access. Users aware that monitoring tools are being used to detect unauthorized use.
7	Rule base Social System	Networking issues	Investigate ways to ensure that commercially available components, public networks like the Internet, or available enterprise systems can be implemented without jeopardizing security or reliability.
8		Quality assurance	Security metrics can be used during the software development lifecycle to eliminate vulnerabilities, particularly during code production, by performing functions such as measuring adherence to secure coding standards, identifying likely vulnerabilities.
9		Mature or proprietary protocols	Immature or proprietary protocols may not be adequately tested either against inadvertent compromises or deliberate attacks. This may leave the interface with more vulnerabilities than if a more mature protocol were used.
10	Strategic System	Cryptography and key management	To enable key management on a scale involving, potentially, tens of millions of credentials and keys as well as local cryptographic processing on the sensors such as encryption and digital signatures.
11		Reliable systems level	Where research on a number of related topics is required to further approaches to building advanced protection architecture that can evolve and can tolerate failures, perhaps of a significant subset of constituents.
12		Strategic support	Assessments of security properties can be used to aid different kinds of decision making, such as program planning, resource allocation, and product and service selection.
13		Security in wireless media	Wireless media may necessitate specific types of security technologies to address wireless vulnerabilities across the wireless path.
14	Hardware	Reliable device level	Efforts to devise cost-effective, tamper-resistant architectures for smart meters and other components, which are necessary for systems-level survivability and resiliency and for improving intrusion detection in embedded systems.
15		High bandwidth of communications channels	Severely-limited bandwidth may constrain the types of security technologies that should be used across an interface while still meeting that interface' s performance requirements.
16		Microprocessor perform memory and compute capabilities	Severely-limited memory and/or compute capabilities of a microprocessor-based platform may constrain the types of security technologies, such as cryptography, that may be used while still allowing the platform to meet its performance requirements.

4.2 Questionnaire Construction

Preferences questionnaires with questions that measures separate variables were adopted to generate the bounded questionnaire where the respondent was presented with a continuous likert scale. A non-comparative likert scaling

techniques was used. The level of measurement of a variable in mathematics and statistics was a classification that was proposed in order to describe the nature of information contained within numbers assigned to objects and, therefore, within the variable.
The questionnaire was divided into two sections:

1. Consumer's perception on Consumer Requirements Model
2. Demography

The respondent was asked to indicate his or her degree of agreement with the statement or any kind of subjective or objective evaluation of the statement. In Section 1, a five-point likert scale was used, rating value from strongly agreed, agreed, neutral, disagreed, and strongly disagreed. The questions comprised sixteen elements such as confidentiality, integrity, availability, privacy concern, tactical oversight monitoring system, facilities misuse prevention, networking issues, quality assurance, mature or proprietary protocols, cryptography and key management, reliable system level, strategy support, security in wireless media reliable device level, high bandwidth of communication channels, and microprocessor perform memory and compute capabilities. The demography variables measured at a nominal level in Section 2 included information on area of research interest and countries.

4.3 Data Distribution and Collection

50 sets of questionnaire were distributed via international workshop, email and peer groups. The selection of the respondents was carefully done based on respondents who possesses limited or more knowledge on the subject of smart grid and its information security. The unreturned questionnaire recorded 7sets; returned usable questionnaire recorded 38; and the returned un-usable questionnaire recorded 5. Figure 3 showed the work flow of questionnaire development, distribution, collection and analysis. Each of the transaction numbers were recorded for back-up references. The returned usable 38 set questionnaires were used to generate analysis.

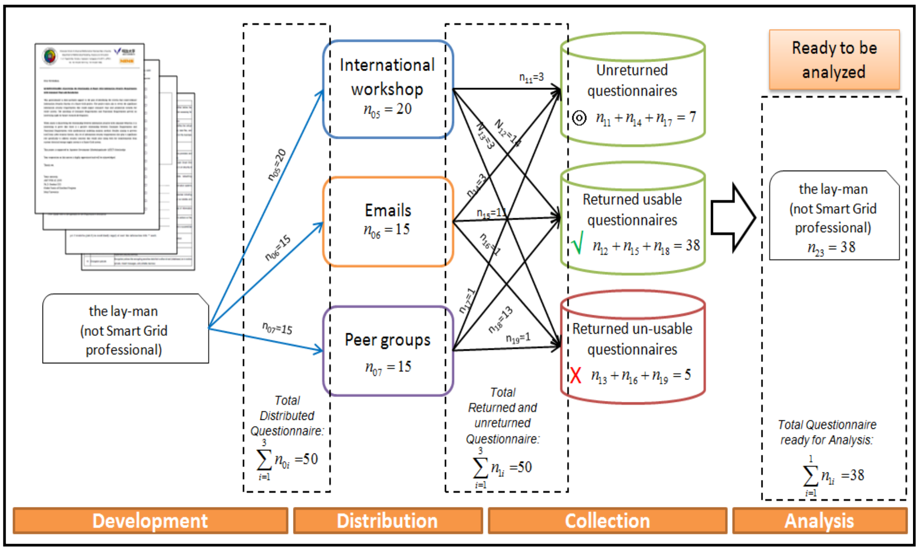

International workshop $n_{05} = 20$
Emails $n_{06} = 15$
Peer groups $n_{07} = 15$
the lay-man (not Smart Grid professional)
n_{05}=20
n_{06}=15
n_{07}=15
Total Distributed Questionnaire: $\sum_{i=1}^{3} n_{0i} = 50$
n_{11}=3
N_{12}=14
N_{13}=3
n_{14}=3
n_{15}=11
n_{16}=1
n_{17}=1
n_{18}=13
n_{19}=1
Total Returned and unreturned Questionnaire: $\sum_{i=1}^{3} n_{1i} = 50$
Unreturned questionnaires ◎ $n_{11} + n_{14} + n_{17} = 7$
Returned usable questionnaires ✓ $n_{12} + n_{15} + n_{18} = 38$
Returned un-usable questionnaires ✗ $n_{13} + n_{16} + n_{19} = 5$
Ready to be analyzed
the lay-man (not Smart Grid professional) $n_{23} = 38$
Total Questionnaire ready for Analysis: $\sum_{i=1}^{1} n_{1i} = 38$
Development
Distribution
Collection
Analysis

Figure. 3. Questionnaire Development, Distribution, Collection and Analysis.

.4 Data Analysis

4.4.1 Descriptive Statistic and Ranking of Variable

Descriptive statistics was adopted as the main methodology for analysis [18]. Correlation was used to analyze statistical relationships between the consumer requirements' variables with the data provided from the questionnaires collected to indicate a predictive relationship that can be exploited in practice.
Minitab was employed to enhance the mathematical calculation to validate the effects of the importance of the consumer of the information security in a smart grid system. Variables of requirements were evaluated one by one so that a ranking has to be chosen by considering only the mean value from the result of descriptive analysis of the raw data obtained from the returned questionnaire.

4.4.2 Histogram and Individual Value Plot versus Country

Histogram is useful in visualizing the consensus of the respondents in this paper such as distribution and data trend. We proposed to adopt histogram method for the decision making to support the hypothesis [19]. Individual value plot was employed to set the appropriate course for the analysis and displayed all data values for small amounts of data. The data collected from different country was been analyzed on the respondents perception on their agreement on the selected consumer requirements.

4.4.3 Chi Square Test (x^2 Test)

x^2 Test was employed as the statistical hypothesis test for the reason of our sampling distribution of the test was a chi-square distribution and the sampling distribution can be made to approximate a chi-square distribution as closely as desired by making the sample size large enough [20].

4.4.4 Pearson Correlation and Degree of Correlation

To obtain the optimal result with respect to the Pearson correlation, we use the Minitab software to generate its output value with the analysis of the respective 16 requirements. An assumption of value lower than 0.5 has low correlation was necessary to analyze and find out which variable is not correlated to one another or having a low correlation relationship to other variable. The Pearson correlation data was used to evaluate the correlation degree and it was defined as strong-normal-weak where S: Strong ($\geq$ 0.6), N: Normal (0.4-0.6) and W: Weak ($\leq$ 0.4).

4.4.5 Lexicographical Order

The output value of Pearson correlation was employed to rank the variables using the lexicographical order methodology. An important property of the lexicographical order in this paper is that it preserves well-orders, when applied to permutations, lexicographic order is increasing numerical order [21].

4.4.6 Network Relationship Ring, Cluster and Tree

Correlation strength was evaluated through stimulation with a wide range of raw data, by varying the network size, number of variables, and the mean values using the Cytoscape software. The network relationship ring achieved two objectives: Firstly to minimize the maximum nodal degree and eliminate low correlated variables, and secondly to minimize the total degree over all network nodes to find strong correlation between variables. Then the network was divided into two clusters and a tree to demonstrate the correlation relationship of the variables perceived by consumers.

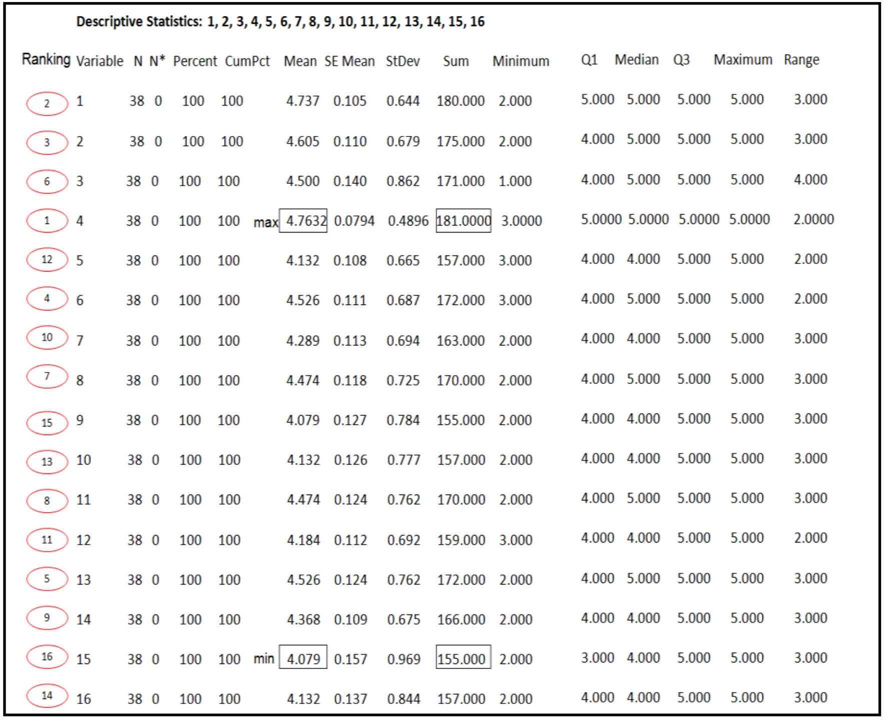
V. RESULTS

5.1 Descriptive Statistics

This part of analysis quantitatively described the main features of the collected data and provided a snap shot of the situation under this study. The descriptive statistics chosen include: N, N*, Percent, CumPct, Mean, SE Mean, Standard Deviation (StDev), Sum, Minimum, Q1, Median, Q3, Maximum, and Range. N was used to track down if any cases were being lost between variables.

Focused on the mean showed in table 3, variable four had the highest mean of 4.7632, which means most of the respondents favor and perceived that variable four had the essentiality as a requirement for a sustainable information security system. On the other hand, tracing variable fifteen, it had the lowest mean of 4.079; this could be one of the less important requirement contributes to the sustainable of the information security in a smart rid system. Where both variable having the same mean, standard deviation (StDev) was taken into account where lower value of StDev rank higher.

Table 3. Descriptive Statistic Table



Descriptive Statistics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

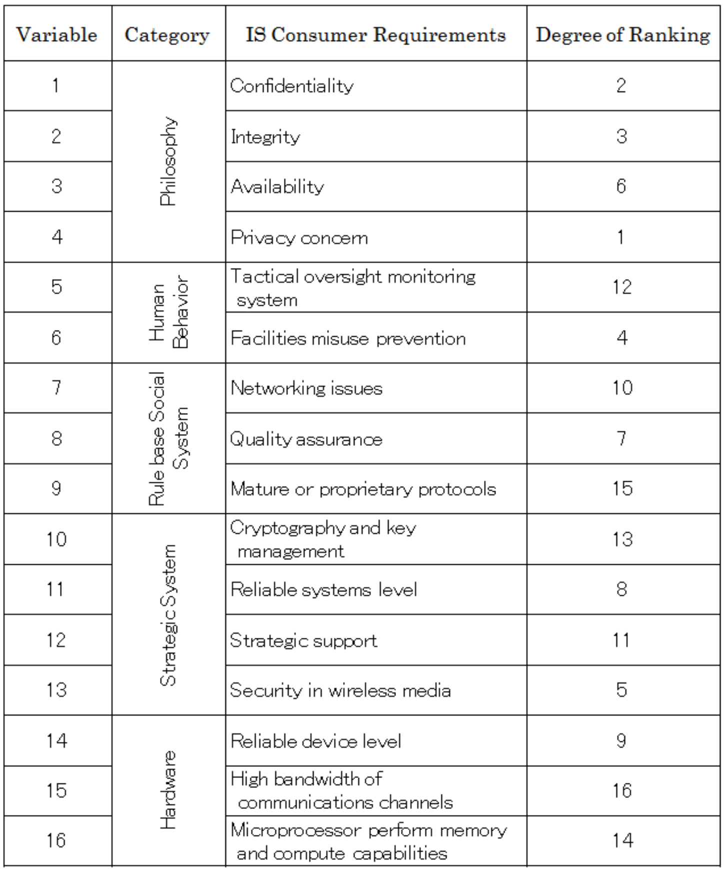
Ranking	Variable	N	N*	Percent	CumPct		Mean	SE Mean	StDev	Sum	Minimum	Q1	Median	Q3	Maximum	Range
2	1	38	0	100	100		4.737	0.105	0.644	180.000	2.000	5.000	5.000	5.000	5.000	3.000
3	2	38	0	100	100		4.605	0.110	0.679	175.000	2.000	4.000	5.000	5.000	5.000	3.000
6	3	38	0	100	100		4.500	0.140	0.862	171.000	1.000	4.000	5.000	5.000	5.000	4.000
1	4	38	0	100	100	max	4.7632	0.0794	0.4896	181.0000	3.0000	5.0000	5.0000	5.0000	5.0000	2.0000
12	5	38	0	100	100		4.132	0.108	0.665	157.000	3.000	4.000	4.000	5.000	5.000	2.000
4	6	38	0	100	100		4.526	0.111	0.687	172.000	3.000	4.000	5.000	5.000	5.000	2.000
10	7	38	0	100	100		4.289	0.113	0.694	163.000	2.000	4.000	4.000	5.000	5.000	3.000
7	8	38	0	100	100		4.474	0.118	0.725	170.000	2.000	4.000	5.000	5.000	5.000	3.000
15	9	38	0	100	100		4.079	0.127	0.784	155.000	2.000	4.000	4.000	5.000	5.000	3.000
13	10	38	0	100	100		4.132	0.126	0.777	157.000	2.000	4.000	4.000	5.000	5.000	3.000
8	11	38	0	100	100		4.474	0.124	0.762	170.000	2.000	4.000	5.000	5.000	5.000	3.000
11	12	38	0	100	100		4.184	0.112	0.692	159.000	3.000	4.000	4.000	5.000	5.000	2.000
5	13	38	0	100	100		4.526	0.124	0.762	172.000	2.000	4.000	5.000	5.000	5.000	3.000
9	14	38	0	100	100		4.368	0.109	0.675	166.000	2.000	4.000	4.000	5.000	5.000	3.000
16	15	38	0	100	100	min	4.079	0.157	0.969	155.000	2.000	3.000	4.000	5.000	5.000	3.000
14	16	38	0	100	100		4.132	0.137	0.844	157.000	2.000	4.000	4.000	5.000	5.000	3.000

Terms in the output and some definitions
N = number of data items in the sample
N* = number of items in the sample that have missing values
Mean = average
Median = 50th percentile
TrMean= the 5% trimmed mean
StDev = standard deviation
SE Mean = standard error of the mean = standard deviation divided by the square root of the sample size
Minimum = smallest data value
Maximum = largest data value
Q1 = 25th percentile = first quartile
Q3 = 75th percentile = third quartile

5.2 Ranking of Variable: Information Security Consumer Requirement

The consumer requirements from table 2 were numbered after the variables' rank referred to the result from Descriptive Statistics analysis, as showed in table 4.

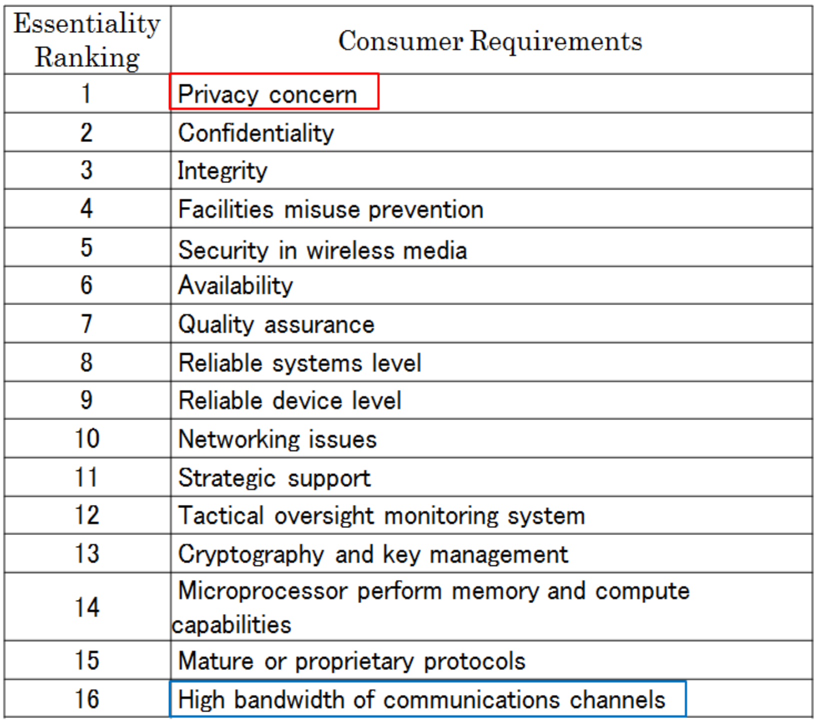
Table 4. Information Security Consumer Requirement



Variable	Category	IS Consumer Requirements	Degree of Ranking
1	Philosophy	Confidentiality	2
2		Integrity	3
3		Availability	6
4		Privacy concern	1
5	Human Behavior	Tactical oversight monitoring system	12
6		Facilities misuse prevention	4
7	Rule base Social System	Networking issues	10
8		Quality assurance	7
9		Mature or proprietary protocols	15
10	Strategic System	Cryptography and key management	13
11		Reliable systems level	8
12		Strategic support	11
13		Security in wireless media	5
14	Hardware	Reliable device level	9
15		High bandwidth of communications channels	16
16		Microprocessor perform memory and compute capabilities	14

Then all the requirements were then again rearranged according to the ranked number, as in table 5. Now, the essentiality ranking of the consumer requirements was clearly displayed in a column. Privacy concern apparently has the potential to become the most important element in among the other fifteen requirements in terms of information security in a smart grid system and high bandwidth of communications channels ranked last.

Table 5. Essentiality Ranking of Information Security Consumer Requirement



Essentiality Ranking	Consumer Requirements
1	Privacy concern
2	Confidentiality
3	Integrity
4	Facilities misuse prevention
5	Security in wireless media
6	Availability
7	Quality assurance
8	Reliable systems level
9	Reliable device level
10	Networking issues
11	Strategic support
12	Tactical oversight monitoring system
13	Cryptography and key management
14	Microprocessor perform memory and compute capabilities
15	Mature or proprietary protocols
16	High bandwidth of communications channels

Comparison was made between table 4 and table 5, the result showed that each of the ranking was a mixture of from five categories of philosophy, human behavior, rule based social system, strategic system and hardware, and hence each category could be concluded to have a balance value of essentiality.

5.3 Histogram

Figure 4 graphically represented a visual impression of the distribution of data and an estimate of the probability distribution of a continuous variable, showed the distribution of a quantitative variable by its relative frequency of data points in an interval. The result output presented a bell-curve slanting to the right, fitting the normal distribution. There was no strong deviation from the distribution, and there was adequate data cleaning. This indicated that the average respondents was at least ticking the value of more than average, that was on agreed or strongly agreed side when asked about the importance of identified requirement in conjunction to the information security in a smart grid system.

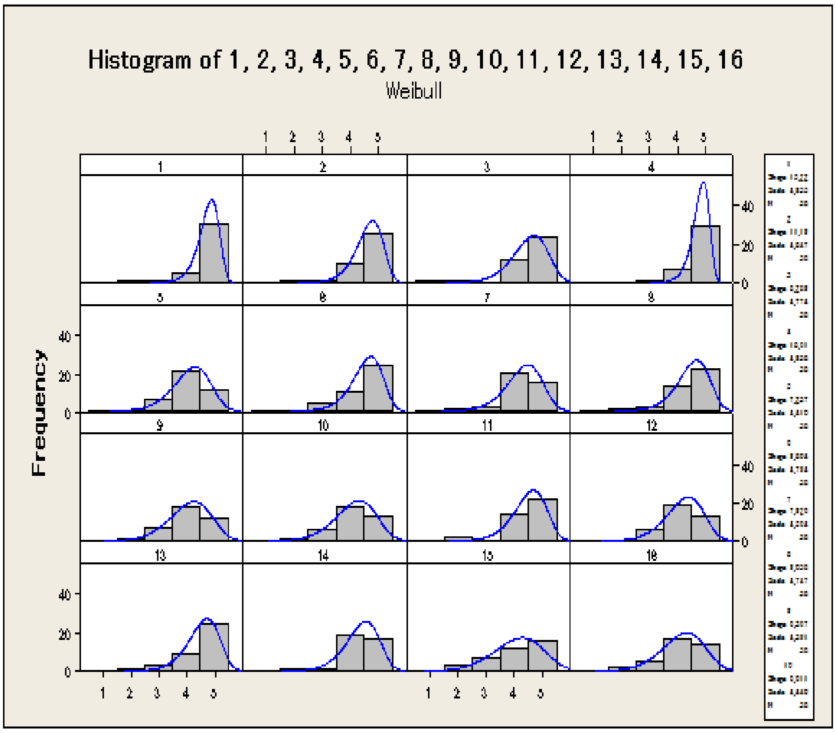


Figure. 4. Histogram.

5.4 Chi-Square Test

To prove that all variables are slanted to the right, we made hypothesis as per below and tested it with Chi-Square test. Hypothesis was stated as per below:

Null Hypothesis
H_o = All 16 graph of variables is as expected value
*Explanation = All identified information security consumer requirements are important

Alternative Hypothesis
H_1= Not all 16 graph of variables slant to the right
*Explanation = Not all identified information security consumer requirements are important
Functions are defined as follow:

f_α : Total number from the sample which chosen answer 1, 2 and 3.

f_β : Total number from the sample which chosen answer 4 and 5.

p_α : Expected percentage of the answer 1, 2 and 3.

p_β : Expected percentage of the answer 4 and 5.

The philosophy and strategy of management with regard to information security is the perfect standard against which technology and other security mechanisms can be measured [22]. Due to this reason, we considered the null hypothesis for philosophy category as $p_\beta = 0.95$ slightly higher than the rest category as $p_\beta = 0.85$.

5.4.1 Chi-square test for the class of "Philosophy" (Variable 1-4)

For the class of "Philosophy", we considered the null hypothesis as following

$$H_0 : p_\alpha = 0.05, \quad p_\beta = 0.95 .$$

The formula of Chi-square test [20] is

$$\chi^2 = \frac{(f_\alpha - n * p_\alpha)^2}{n * p_\alpha} + \frac{(f_\beta - n * p_\beta)^2}{n * p_\beta}$$

Table 6. Chi-Square Test for the Class of "Philosophy" (Variable 1)

f_α	f_β	$n * p_\alpha$	$n * p_\beta$	χ^2
2	36	1.9	36.1	0.0055

Chi-square value χ^2 =0.0055 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 7. Chi-Square Test for the Class of "Philosophy" (Variable 2)

f_α	f_β	$n * p_\alpha$	$n * p_\beta$	χ^2
2	36	1.9	36.1	0.0055

Chi-square value χ^2 =0.0055 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 8. Chi-Square Test for the Class of "Philosophy" (Variable 3)

f_α	f_β	$n * p_\alpha$	$n * p_\beta$	χ^2
2	36	1.9	36.1	0.0055

Chi-square value χ^2 =0.0055 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 9. Chi-Square Test for the Class of "Philosophy" (Variable 4)

f_α	f_β	$n * p_\alpha$	$n * p_\beta$	χ^2
1	37	1.9	36.1	0.4488

Chi-square value χ^2 =0.4488 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

5.4.2 Chi-square test for the class of "Human behavior" (Variable 5-6)

For the class of "Human behavior", we considered the null hypothesis as following

$$H_0 : p_\alpha = 0.15, \quad p_\beta = 0.85 .$$

The formula of Chi-square test is

$$\chi^2 = \frac{(f_\alpha - n * p_\alpha)^2}{n * p_\alpha} + \frac{(f_\beta - n * p_\beta)^2}{n * p_\beta}$$

Table 10. Chi-Square Test for the Class of "Human Behaviour" (Variable 5)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
5	33	5.7	32.3	0.1011

Chi-square value $\chi^2 = 0.1011 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 11. Chi-Square Test for the Class of “Human Behaviour” (Variable 6)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
4	34	5.7	32.3	0.5965

Chi-square value $\chi^2 = 0.5965 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

5.4.3 Chi-square test for the class of “Rule based on social system” (Variable 7-9)

For the class of “Rule based on social system”, we considered the null hypothesis as following

$$H_0 : p_\alpha = 0.15, \quad p_\beta = 0.85.$$

The formula of Chi-square test is

$$\chi^2 = \frac{(f_\alpha - n*p_\alpha)^2}{n*p_\alpha} + \frac{(f_\beta - n*p_\beta)^2}{n*p_\beta}$$

Table 12. Chi-Square Test for the Class of “Rule Based on Social System” (Variable 7)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
3	35	5.7	32.3	1.5046

Chi-square value $\chi^2 = 1.5046 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 13. Chi-Square Test for the Class of “Rule Based on Social System” (Variable 8)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
3	35	5.7	32.3	1.5046

Chi-square value $\chi^2 = 1.5046 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 14. Chi-Square Test for the Class of “Rule Based on Social System” (Variable 9)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
8	30	5.7	32.3	1.0918

Chi-square value $\chi^2 = 1.0918 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

5.4.4 Chi-square test for the class of “Strategic system” (Variable 10-13)

For the class of “Strategic system”, we considered the null hypothesis as following

$$H_0 : p_\alpha = 0.15, \quad p_\beta = 0.85.$$

The formula of Chi-square test is

$$\chi^2 = \frac{(f_\alpha - n*p_\alpha)^2}{n*p_\alpha} + \frac{(f_\beta - n*p_\beta)^2}{n*p_\beta}$$

Table 15. Chi-Square Test for the Class of “Strategic System” (Variable 10)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
7	31	5.7	32.3	0.3488

Chi-square value $\chi^2 = 0.3488 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 16. Chi-Square Test for the Class of “Strategic System” (Variable 11)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
3	36	5.7	32.3	2.8256

Chi-square value $\chi^2 = 2.8256 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 17. Chi-Square Test for the Class of “Strategic System” (Variable 12)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
6	32	5.7	32.3	1.0186

Chi-square value $\chi^2 = 0.0186 < 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 18. Chi-Square Test for the Class of "Strategic System" (Variable 13)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
4	34	5.7	32.3	0.5965

Chi-square value χ^2 =0.5965 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

5.4.5 Chi-square test for the class of "Hardware" (Variable 14-16)

For the class of "Hardware", we considered the null hypothesis as following

$$H_0 : p_\alpha = 0.15, \quad p_\beta = 0.85 .$$

The formula of Chi-square test is

$$\chi^2 = \frac{(f_\alpha - n*p_\alpha)^2}{n*p_\alpha} + \frac{(f_\beta - n*p_\beta)^2}{n*p_\beta}$$

Table 19. Chi-Square Test for the Class of "Hardware" (Variable 14)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
2	36	5.7	32.3	2.8256

Chi-square value χ^2 =2.8256 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 20. Chi-Square Test for the Class of "Hardware" (Variable 15)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
10	28	5.7	32.3	3.8163

Chi-square value χ^2 =3.8163 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

Table 21. Chi-Square Test for the Class of "Hardware" (Variable 16)

f_α	f_β	$n*p_\alpha$	$n*p_\beta$	χ^2
7	31	5.7	32.3	0,3488

Chi-square value χ^2 =0.3488 $< 3.841 = \chi^2_{0.05,1}$, the hypothesis H_0 was not rejected.

From the result above, we concluded that the entire null hypothesis from each class has not been rejected. Also, we obtained the following result:

$$p_\beta > 0.8$$

This means that results of p_β showed that the value is greater than 80% of the entire respondents' agreement on the essentiality of the consumer requirements identified. Therefore, this result supported our null hypothesis that the graphs of all of the variables are slanted to the right.

In conclusion, the null hypothesis was not rejected.

5.5 Individual Value Plot versus Country

There were respondents from 14 countries took part in the questionnaire activity. Individual value plot versus country were accomplished in purpose to identify the difference of perception of consumers from different countries, as showed in figure 5.

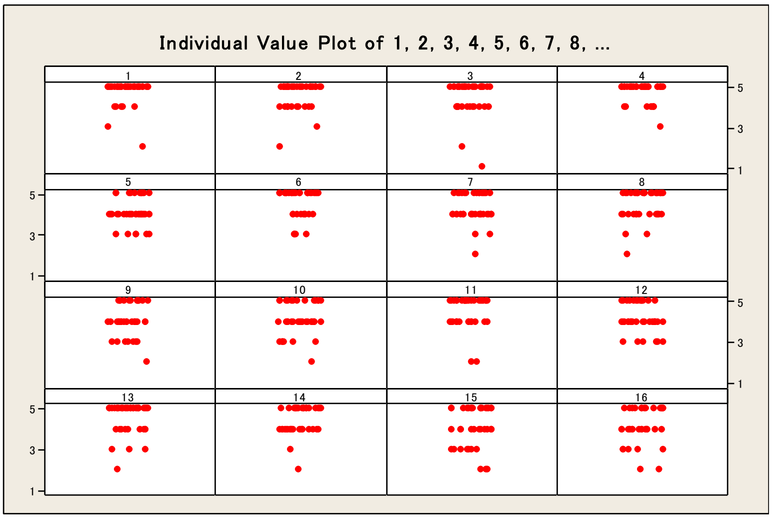


Figure. 5. Summary of Individual Value Plot versus Countries.

5.5.1 Confidentiality versus Country

Figure 6 showed most of the countries strongly agreed that confidentiality was essential for a sustainable information security system in a smart grid; there was a dot on value 2 for the country of China. This could be due to the confidentiality in China has been a volatile for the country.

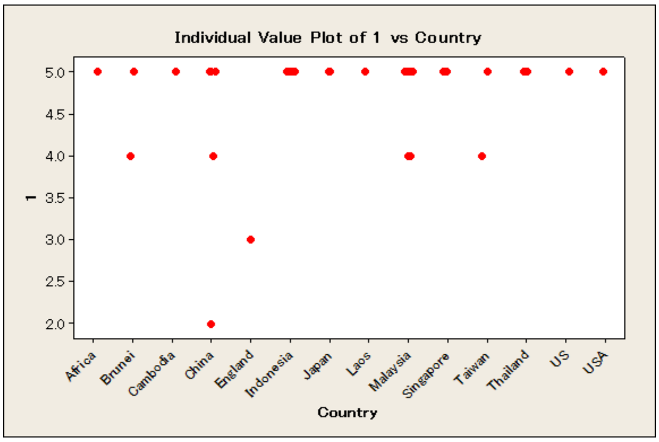


Figure. 6. Individual Value Plot of Confidentiality versus Countries.

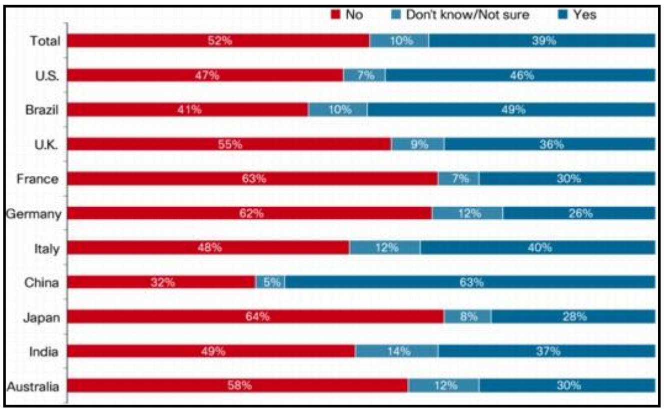


Figure 7 showed the number of times IT has had to deal with an employee for accessing unauthorized networks or facilities:

Figure. 7. Employee Accessed Unauthorized Networks or Facilities.

39 percent of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility, with almost half of IT professionals reporting this in Brazil (49 percent) and the United States (46 percent), and 63 percent in China [23]. This could support on the dot on value 2 for China being stating that confidentiality was not so important contribute towards the sustainability of an information security in a smart grid system.

5.5.2 Reliable systems level versus Country

Among the thirty eight respondents, only two, from China and Taiwan, disagreed where research on a number of related topics was required to further approaches to building advanced protection architecture that can evolve and can tolerate failures, as showed in figure 8. This might due to the rapidly growing economies like China and Taiwan have different smart grid infrastructure needs from those of OECD countries [24].

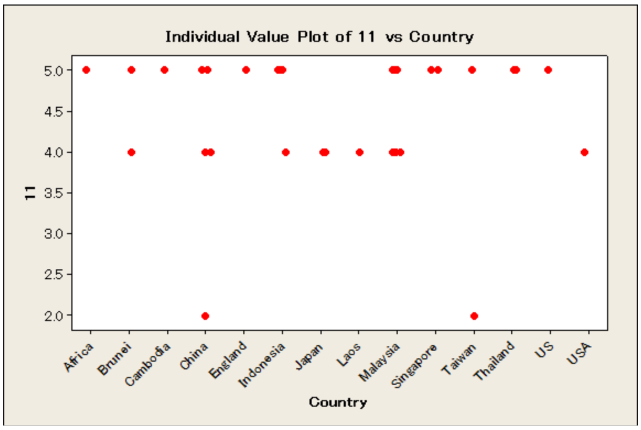


Figure. 8. Value Plot of Reliable systems level versus Countries.

5.5.3 Microprocessor performs memory and compute capabilities versus Country

There were relatively 5 respondents choose to be in neutral and two from Malaysia and Taiwan were disagreed that microprocessor performs memory and compute capabilities was an essential element for an information security in a smart grid system, as showed in figure 9.

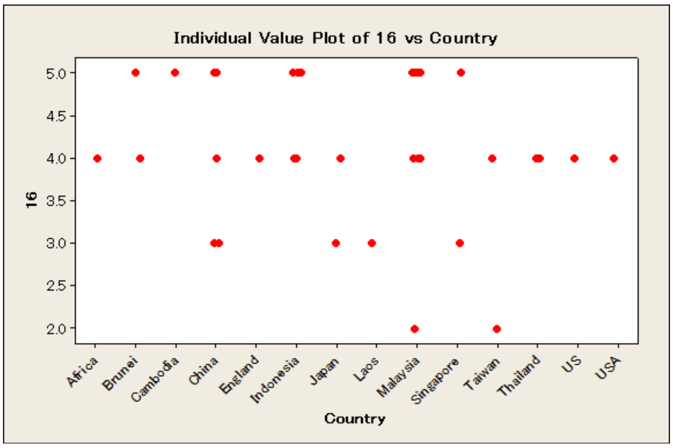
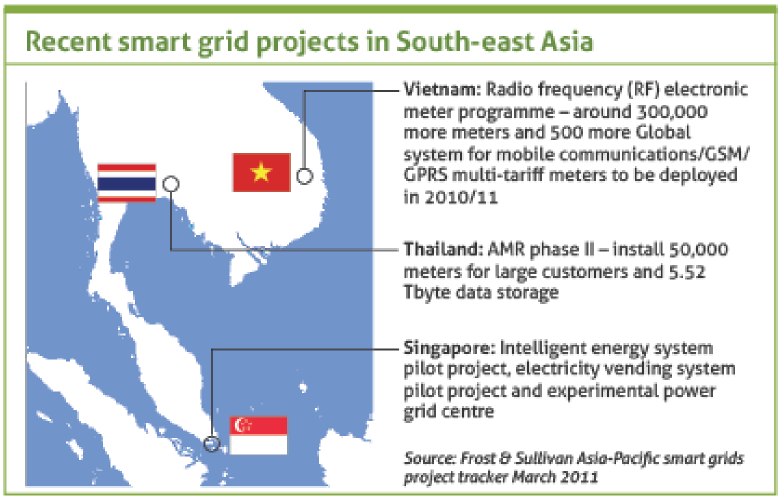


Figure. 9. Value Plot of Microprocessor performs memory and compute capabilities versus Countries.

Recent smart grid projects in South-east Asia



Vietnam: Radio frequency (RF) electronic meter programme – around 300,000 more meters and 500 more Global system for mobile communications/GSM/ GPRS multi-tariff meters to be deployed in 2010/11

Thailand: AMR phase II – install 50,000 meters for large customers and 5.52 Tbyte data storage

Singapore: Intelligent energy system pilot project, electricity vending system pilot project and experimental power grid centre

Source: Frost & Sullivan Asia-Pacific smart grids project tracker March 2011

Figure. 10. Recent Smart Grid Projects in South-east Asia.

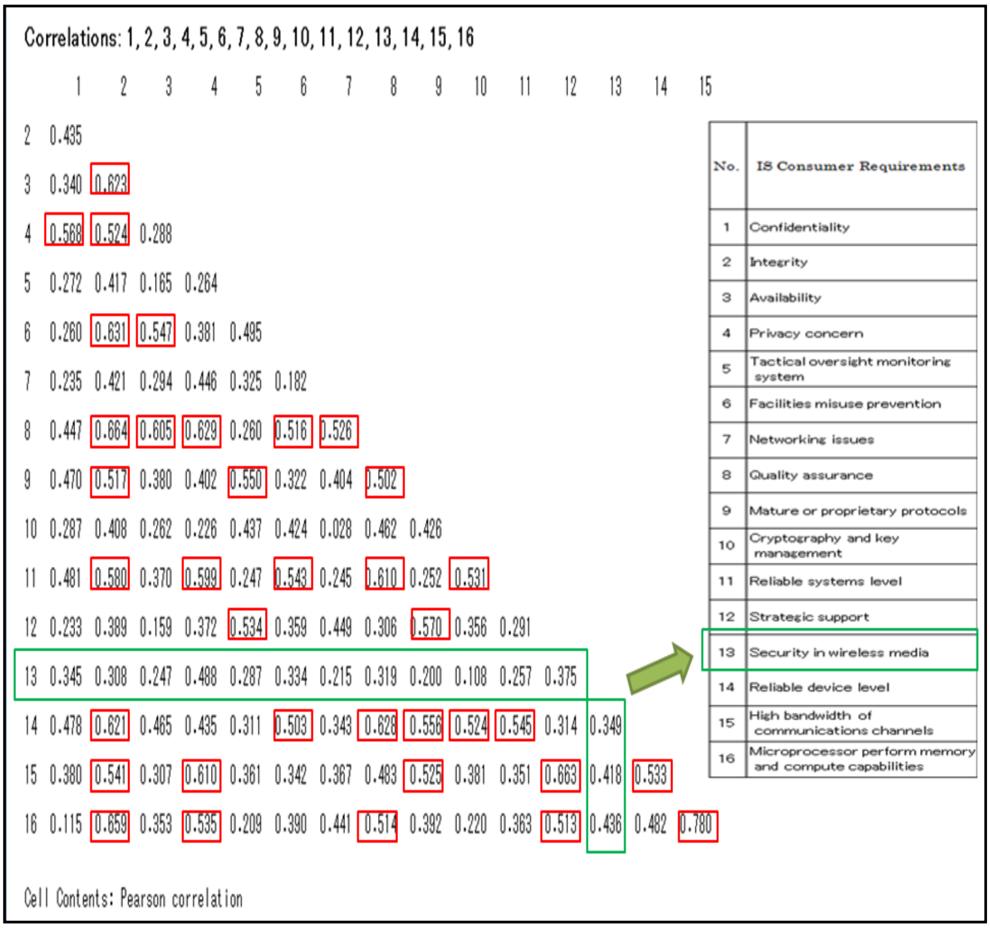
Malaysia is a developing country and was being lobbied recently to develop a roadmap and institutional framework to ensure coordinated efforts for the long-term. Figure 10 showed the recent smart grid projects in South-east Asia [25]. The respondent might not aware of the importance of what the microprocessor performs memory and compute capabilities could bring effect to the system. As for Taiwan, it is the home to the world's largest contract manufacturing firms, accounting for 65% of the world's Electronics Manufacturing Services business [26]. Taiwan has already made the semiconductor industry akin to the contract manufacturing industry, thus the quality of microprocessor is assured.

In conclusion, the result of individual value plot versus country shows that there are still minority respondents stating that confidentiality is not so important contribute towards the sustainability of an information security in a smart grid system, disagreed where research on a number of related topics was required to further approaches to building advanced protection architecture that can evolve and can tolerate failures, and disagreed that microprocessor performs memory and compute capabilities was an essential element for an information security in a smart grid system. This might due to the rapidly growing economies in different countries have different smart grid infrastructure needs.

5.6 Pearson Correlation

In this section, we examined the relationship between two variables. The Pearson Correlation was employed in the computation process. Result in figure 11 showed that most of the variable of the requirements were positive correlated to each other. Variable 13, security in wireless media, seems to have no strong correlation with other fifteen variables. This could be due to its entertainment element contributed less relationship with other information security requirement although the essentiality of security in wireless media was essential.

There was some reason supported this findings. Wireless networks offer great potential for exploitation for two reasons; they use the airwaves for communication, and wireless-enabled laptops are ubiquitous. Several security protocols designed for wired-line networks have been adopted for use in wireless networks. However, they may not be suitable for wireless networks and devices since scenarios and capabilities applicable to wired-line networks may not be valid in wireless networks [27]. Most security technologies are currently deployed in wired networks and are not fully applicable to wireless networks involving mobile devices with limited computing capability [28].



```
Correlations: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

       1      2      3      4      5      6      7      8      9      10     11     12     13     14     15
2   0.435
3   0.340  0.623
4   0.568  0.524  0.288
5   0.272  0.417  0.165  0.264
6   0.260  0.631  0.547  0.381  0.495
7   0.235  0.421  0.294  0.446  0.325  0.182
8   0.447  0.664  0.605  0.629  0.260  0.516  0.526
9   0.470  0.517  0.380  0.402  0.550  0.322  0.404  0.502
10  0.287  0.408  0.262  0.226  0.437  0.424  0.028  0.462  0.426
11  0.481  0.580  0.370  0.599  0.247  0.543  0.245  0.610  0.252  0.531
12  0.233  0.389  0.159  0.372  0.534  0.359  0.449  0.306  0.570  0.356  0.291
13  0.345  0.308  0.247  0.488  0.287  0.334  0.215  0.319  0.200  0.108  0.257  0.375
14  0.478  0.621  0.465  0.435  0.311  0.503  0.343  0.628  0.556  0.524  0.545  0.314  0.349
15  0.380  0.541  0.307  0.610  0.361  0.342  0.367  0.483  0.525  0.381  0.351  0.663  0.418  0.533
16  0.115  0.659  0.353  0.535  0.209  0.390  0.441  0.514  0.392  0.220  0.363  0.513  0.436  0.482  0.780

Cell Contents: Pearson correlation
```

No.	IS Consumer Requirements
1	Confidentiality
2	Integrity
3	Availability
4	Privacy concern
5	Tactical oversight monitoring system
6	Facilities misuse prevention
7	Networking issues
8	Quality assurance
9	Mature or proprietary protocols
10	Cryptography and key management
11	Reliable systems level
12	Strategic support
13	Security in wireless media
14	Reliable device level
15	High bandwidth of communications channels
16	Microprocessor perform memory and compute capabilities

Figure. 11. Pearson Correlation Test with P-value test.

In conclusion, we could see that the wireless connections have become an increasingly popular way of providing internet access although it is still in its development process. When the wireless becomes a common method for data transmission especially from the smart meter to the grid, security becomes a highly important part of the wireless network structure. Hence, although the security in wireless media is not correlated to other variable tested, it is still an important asset for all systems using a wireless network.

5.6.1 Degree of Correlation

The degree of correlation analysis was worked out to consider how strong or how weak each pair of tested variables were correlated among each other, as showed in table 22. We fixed three categories explicating strong, normal and weak for each pair of tested variables, as per below.

S: Strong (≥ 0.6)
N: Normal (0.4-0.6)
W: Weak (≤ 0.4).

Table 22. Degree of Correlation Analysis.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		N	W	N	W	W	W	N	N	W	N	W	W	N	W	W
2	N		S	N	N	S	N	S	N	N	N	W	W	S	N	S
3	W	S		W	W	N	W	S	W	W	W	W	W	N	W	W
4	N	N	W		W	W	N	S	N	W	N	W	N	N	S	N
5	W	N	W	W		N	W	W	N	N	W	N	W	W	W	W

6	W	S	N	W	N		W	N	W	N	N	W	W	N	W	W
7	W	N	W	N	W	W		N	N	W	W	N	W	W	W	N
8	N	S	S	S	W	N	N		N	N	S	W	W	S	N	N
9	N	N	W	N	N	W	N	N		N	W	N	W	N	N	W
10	W	N	W	W	N	N	W	N	N		N	W	W	N	W	W
11	N	N	W	N	W	N	W	S	W	N		W	W	N	W	W
12	W	W	W	W	N	W	N	W	N	W	W		W	W	S	N
13	W	W	W	N	W	W	W	W	W	W	W	W		W	N	N
14	N	S	N	N	W	N	W	S	N	N	N	W	W		N	N
15	W	N	W	S	W	W	W	N	N	W	W	S	N	N		S
16	W	S	W	N	W	W	N	N	W	W	W	N	N	N	S	

The accumulated numbers of S, N and W were calculated for each variable and were recorded in table 23.

Table 23. Accumulated Numbers of the Degree of Correlation Analysis.

	S	N	W
1	0	6	9
2	5	8	2
3	2	2	11
4	2	8	5
5	0	5	10
6	1	6	8
7	0	6	9
8	5	7	3
9	0	10	5
10	0	7	8
11	1	6	8
12	1	4	10
13	0	3	12
14	2	9	4
15	3	5	7
16	2	6	7

5.6.2 Lexicographical Order

Upon the completion of table 23, correlation ranking of information security consumer requirements via pearson correlation test observation was generated employing lexicographical order methodology.
Table 23 showed that variable 2 was larger than 8, followed by 15, 14, 4, 16, 3, 11, 6, 12, 9, 10, 1, 7, 5, 13. In the process of calculation, the numbers in S column will be taken to identify which was the largest numbers among the variable which gain most S means it has the strongest correlation value to other pairs of variable being compared. When it comes to same number counted, for example, variable 2 and variable 5 has the same S count of five, and then second column of N will be referred, for this case, N counts of variable 2 was larger than variable 8, so variable 2 was considered to be larger than variable 8.
Lexicographical Ordering was adopted to create result as per below.
Variable 2 > 8 > 15 > 14 > 4 > 16 > 3 > 11 > 6 > 12 > 9 > 10 > 1 > 7 > 5 > 13
A table of correlation ranking of information security consumer requirements via Pearson correlation test observation was developed, as showed in table 24.

Table 24. Table of Correlation Ranking of Information Security Consumer Requirements.

Correlation Ranking	Consumer Requirements
1	Integrity
2	Quality assurance
3	High bandwidth of communications channels
4	Reliable device level
5	Privacy concern
6	Microprocessor perform memory and compute capabilities
7	Availability
8	Reliable systems level
9	Facilities misuse prevention
10	Strategic support
11	Mature or proprietary protocols
12	Cryptography and key management
13	Confidentiality
14	Networking issues
15	Tactical oversight monitoring system
16	Security in wireless media

Table 24 concluded that integrity has the strongest correlation strength with other pair of information security consumer requirement identified, followed by quality assurance, high bandwidth of communication channels, reliable device level, privacy concern, microprocessor perform memory and compute capabilities, availability, reliable system level, facilities misuse prevention, strategy support, mature or proprietary protocols, cryptography and key management, confidentiality, networking issues, tactical oversight monitoring system, and last but not least, security in wireless media.

The purpose of this ranking is to create a picture of a common language and a detailed understanding of the customer's requirements. When a greater importance is placed on consumer retention, the system can be developed to gain their expectations, for an enlightened consumer is an empowered consumer. Instead of adding to the previous debate whether and how many consumers are interested in information security as such, the aim is to provide a deeper investigation into the information cues on security requirements that really attract consumer interest and therefore may merit specific attention in future information security policies. Statistic sometimes shows differences from the theoretical result that we might not know. Based on this study, the result showed that integrity, quality assurance and high bandwidth of communications channels has high correlation with each other. We could conclude that any changes in the unauthorized modification or destruction of information will lead to the changes in the quality assurance performing functions and types of security technologies that should be used across an interface while still meeting that interface's performance requirements.

5.6.3 Correlation Relationship Ring

We study the dynamics of correlation between the variables with different value of threshold. For many such situations, it was found that the correlations between individual variables are better indicators than the value of attributes.

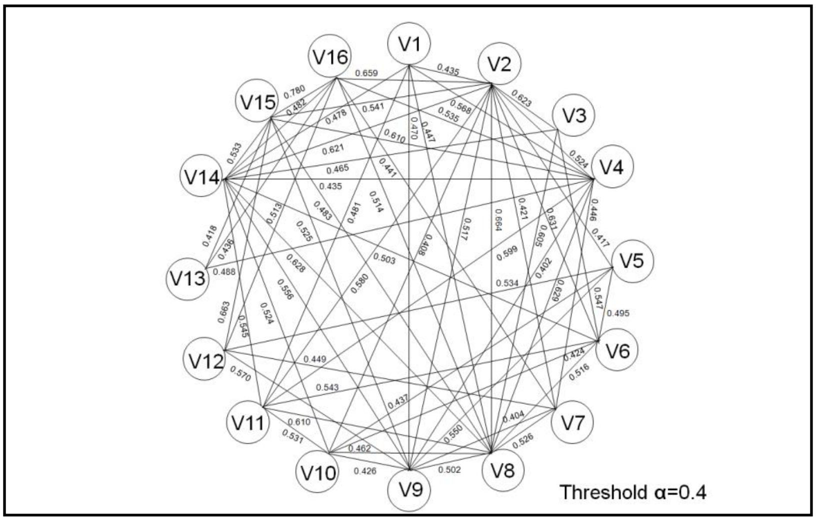


Figure. 12. Correlation Relationship Ring, Threshold α =0.4.

Figure 12 above shows the correlation with the threshold α value of 4.

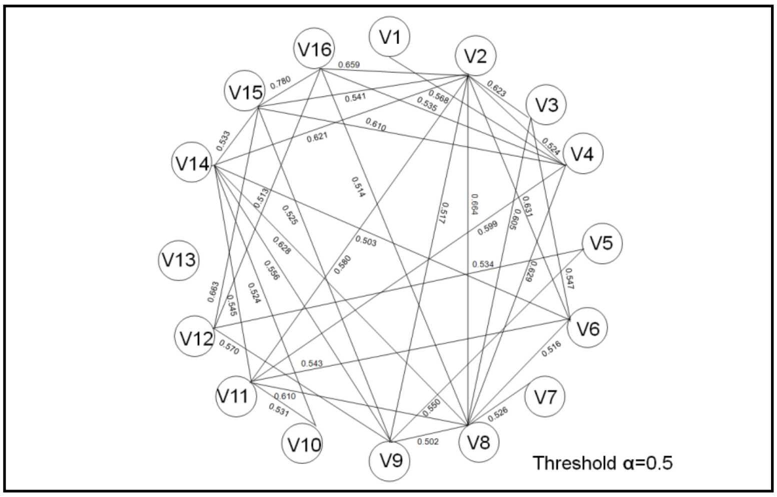


Figure. 13. Correlation Relationship Ring, Threshold α =0.5.

When the threshold was increased gradually, the correlation pattern changed, the correlation lines reduced, as showed in figure 13 and 14.

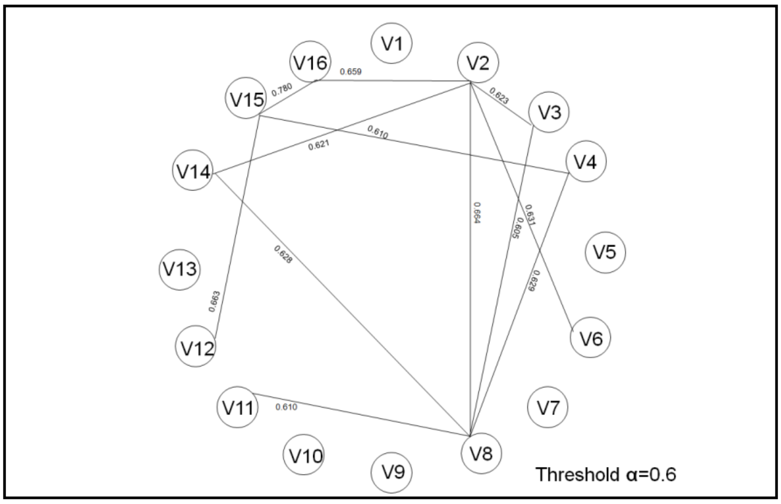


Figure. 14. Correlation Relationship Ring, Threshold α =0.6.

5.6.4 Correlation Relationship Cluster

We cleaned the correlation matrix by setting the threshold value to α =0.6 and α =0.66 in order to create a correlation relationship cluster. In this cluster, we could see that they are group into two strong correlation clusters, as per below figure 15.

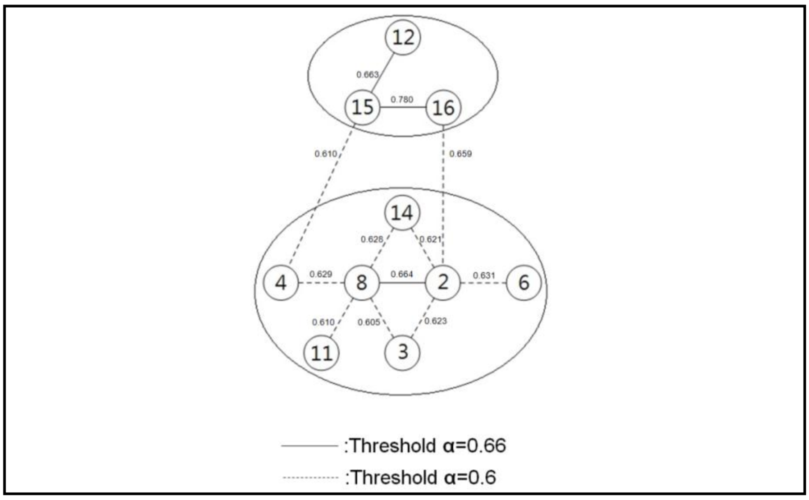


Figure. 15. Correlation Relationship Cluster, Threshold α =0.6, α =0.66.

We cleaned again the correlation matrix by setting the threshold value to α =0.66 in order to create independent correlation relationship clusters.

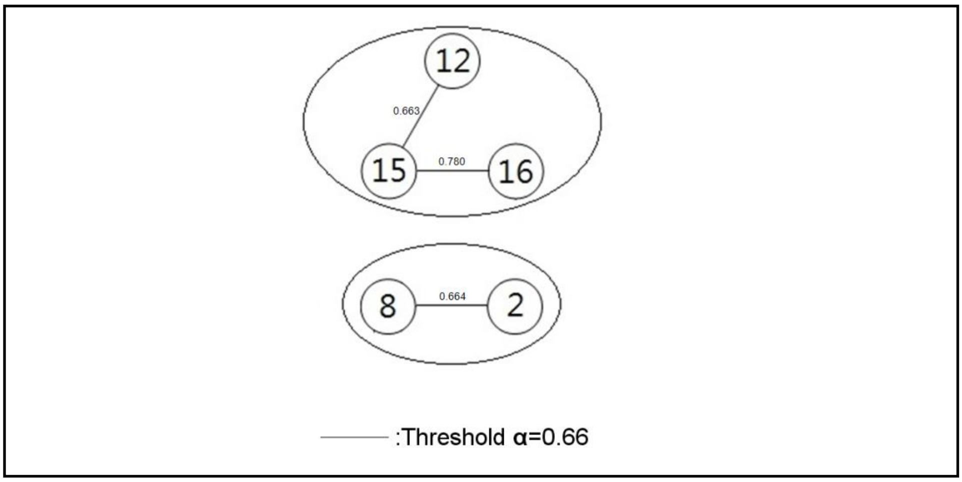


Figure. 16. Correlation Relationship Cluster, Threshold α =0.6.

From figure 16, variable 2 and 8 are integrity and quality assurance. Whereas variable 12, 15 and 16 are strategic support, high bandwidth of communications channels, and microprocessor perform memory and compute capabilities. Because integrity belongs to the category of philosophy, while quality assurance belongs to rule based social system, it supports to the statement that the elements of category philosophy and rule based social system are closely correlated. On the other hand, strategic support belongs to the category of strategic system, while high bandwidth of communications channels, and microprocessor perform memory and compute capabilities belongs to the hardware category, so we could conclude that strategic system and hardware are closely correlated.

5.6.5 **Correlation Relationship Tree**

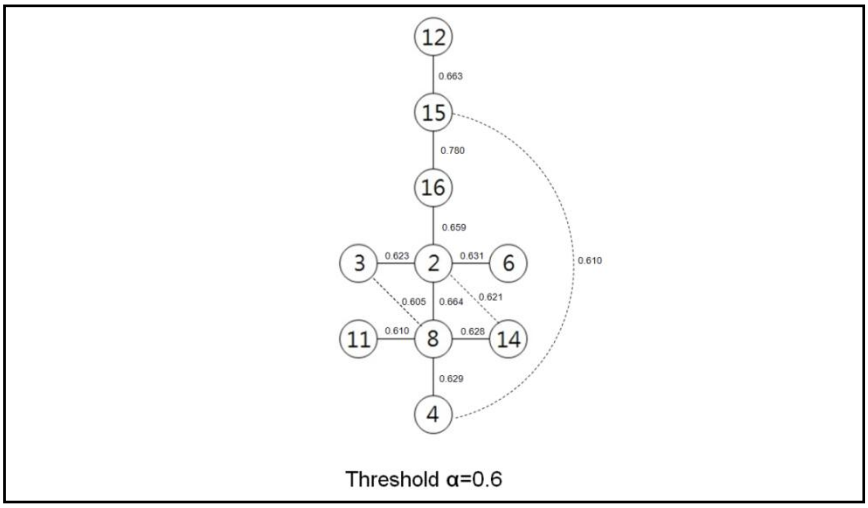


Figure. 17. Correlation Relationship Tree, Threshold α =0.6.

These tree relations enable us to see the main correlation strength, as showed in figure 17. The strongest point was attached between variable 15 (high bandwidth of communication channels) and variable 16 (microprocessor perform memory and compute capabilities). These two variables are from the category of hardware. In conclusion, the items in the hardware category are highly correlated to each other, when a consumer perceived on the hardware supporting the information security system, they perceived them as a package, for they carries the same weight.

VI. CONCLUSION

This paper gives insight into the importance of information security criteria as the main aspect perceived to impact customer trust towards the entire smart grid system. The analysis takes aim at identifying the criteria that could enhance the information security system of a smart grid project and discusses the impact and significance of each of the requirements identified. The major finding of this paper exhibit the agreement from the respondent on the essentiality of the identified sixteen consumer requirements, and the ranking of essentiality of the requirements were generated. The most important consumer requirement of information security in a smart grids system referred to the respondents' respond was privacy concern, followed by confidentiality, integrity, facilities misuse prevention, security in wireless media, availability, quality assurance, reliable systems level, reliable device level, networking issues, strategic support, tactical oversight monitoring system, cryptography and key management, microprocessor perform memory and compute capabilities, mature or proprietary protocols, and high bandwidth of communications channels. Comparison result showed that each of the ranking

was a mixture of from five categories of philosophy, human behavior, rule based social system, strategic system and hardware, and hence each category could be concluded to have a balance value of essentiality.
Histogram test indicated that the average respondents was at least ticking the value of more than average, that was on agreed or strongly agreed side when asked about the importance of identified requirement in conjunction to the information security in a smart grid system.
To prove that all variables are slanted to the right, we made hypothesis and tested it with Chi-Square test. From the result, we concluded that the entire null hypothesis from each class has not been rejected. Also, the results of p_β showed that the value is greater than 80% of the entire respondents' agreement on the essentiality of the consumer requirements identified. Therefore, this result supports our null hypothesis that the graphs of all of the variables are slanted to the right.
Individual value plot versus country shows that there are still minority respondents stating that confidentiality is not so important contribute towards the sustainability of an information security in a smart grid system, disagreed where research on a number of related topics was required to further approaches to building advanced protection architecture that can evolve and can tolerate failures, and disagreed that microprocessor performs memory and compute capabilities was an essential element for an information security in a smart grid system. This might due to the rapidly growing economies in different countries have different smart grid infrastructure needs.
Pearson correlation test showed that security in wireless media has very low correlation with others variable. The wireless connections have become an increasingly popular way of providing internet access although it is still in its development process. When the wireless becomes a common method for data transmission especially from the smart meter to the grid, security becomes a highly important part of the wireless network structure. Hence, although the security in wireless media is not correlated to other variable tested, it is still an important asset for all systems using a wireless network.
Employed the output from the Pearson correlation test, we generated two means of ranking for the variables, the lexicographical order to test the essential variables and the correlation relationship ring, cluster and tree to test the essential category. Lexicographical order test showed that integrity, quality assurance and high bandwidth of communications channels has high correlation with each other. Any changes in the unauthorized modification or destruction of information will lead to the changes in the quality assurance performing functions and types of security technologies that should be used across an interface while still meeting that interface's performance requirements. Correlation relationship ring, cluster and tree concluded that the items in the hardware category are highly correlated to each other, when a consumer perceived on the hardware supporting the information security system, they perceived them as a package, for they carries the same weight.
The success of this effort appeared to hinge on utility companies championing information system security initiatives and propagating an awareness of the importance of information security among consumers at all levels of the community. In this study, there was a causal relationship because consumer requirements cause energy authorities to modify their information security policies according to consumer demand.

VII. DISCUSSION

This paper has tutorial contents where some related backgrounds were provided, especially covering the cyber security requirement of smart grid information infrastructure. It provides a combination of methodologies and a set of sixteen identified information security consumer requirements conceptually as original contributions. This paper aims to contribute a sight for the readers to have a conceptual knowledge of the electric power grid and a better understanding of cyber security, and focuses main on helping the government and utilities provider to enhance processes, to develop and prioritize the necessary requirements for securing their information in a smart grid.

ACKNOWLEDGMENT

The authors wish to thank Dr. Siew Hai Yen, Dr. Shu-ichi Kinoshita, Dr. Akiyasu Tomoeda, Tateno Kurina for the comments; and Professor Masayasu Mimura for mentoring. This study was supported by the Meiji University Global COE Program "Formation and Development of Mathematical Sciences Based on Modeling and Analysis", Meiji Institute for Advanced Study of Mathematical Sciences (MIMS), and the Japanese government's Ministry of Education, Culture, Sports, Science, and Technology (MEXT) scholarship.

REFERENCE AND CITATIONS SECTION

[1] Christoph Weber, Adriaan Perrels, (2000) "Modelling lifestyle effects on energy demand and related emissions", Energy Policy 28, pp. 549-56.

[2] Inge Røpk, (2001) "New technology in everyday life – social processes and environmental impac", Ecological Economics 38, pp. 403–422.

[3] R. Stark, H. Hayka, D. Langenberg, (2009) "New potentials for virtual product creation by utilizing grid technology", CIRP Annals - Manufacturing Technology, Volume 58, Issue 1, Pages 143-146.

[4] Amy Poh Ai Ling, Masao Mukaidono, "Smart Grid Information Security (IS) Functional Requirement", International Journal of Emerging Sciences, Vol.1, No.3, September 2011, pp. 371-386.

[5] Twiki Research 2010, CNSLab (Computer Networks and Security Lab), available at: http://cnslab.snu.ac.kr/twiki/bin/view/Main/Research

[6] Amy Poh Ai Ling, Masao Mukaidono, “Selection of Model in Developing Information Security Criteria on Smart Grid Security System”, Smart Grid Security and Communications, The Ninth International Symposium on Parallel and Distributed Processing with Applications (ISPA), No. 108, May 2011, Korea, pp.91-98; Journal of Convergence, Vol.2, No.1, 2011-6, pp.39-46.

[7] “Information Security Incident Survey Report”, NPO Japan Network Security Association, Security Incident Investigation Working Group, Ver. 1.0, March 31, 2010.

[8] Jean-Philippe Vasseur, Adam Dunkels, (2010) “Smart Grid”, Interconnecting Smart Objects with IP, pp. 305-324.

[9] Leonardo Meeus, Marcelo Saguan, (2011) “Innovating grid regulation to regulate grid innovation: From the Orkney Isles to Kriegers Flak via Italy”, Renewable Energy, Volume 36, Issue 6, June 2011, pp.1761-1765.

[10] Tony Flick, Justin Morehouse, “Smart Grid: What Is It?”, Securing the Smart Grid, 2011, Pages 1-18.

[11] Ravi Akella, Han Tang, Bruce M. McMillin, “Analysis of information flow security in cyber–physical systems”, International Journal of Critical Infrastructure Protection, Volume 3, Issues 3-4, December 2010, Pages 157-173.

[12] G. Laccetti, G. Schmid, (2007) “A framework model for grid security”, Future Generation Computer Systems, Volume 23, Issue 5, June 2007, pp.702-713.

[13] Simon Perry, “Watt matters – smart grid security”, Infosecurity, Volume 6, Issue 5, July-August 2009, Pages 38-40.

[14] Amy Poh Ai Ling, Mukaidono Masao, “Grid Information Security Functional Requirement Fulfilling Information Security of a Smart Grid System”, International Journal of Grid Computing & Applications, Vol. 2, No. 2, June 2011, pp. 1–19.

[15] Walsham, G., (1996) “The emergence of interpretivism in IS research”, Information Systems Research, Vol. 6, pp.376-94.

[16] Klein, H.K., Myers, M.D., (1999) “A set of principles for conducting and evaluating interpretive field studies in information systems”, MIS Quarterly, Vol. 23 pp.67-94.

[17] Ramberg, Bjørn and Kristin Gjesdal (2005) “Hermeneutics”, Stanford Encyclopedia of Philosophy.

[18] Rossi et al., 1992 R.E. Rossi, D.J. Mulla, A.G. Journel and E.H. Franz, Geostatistical tools for modeling and interpreting ecological spatial dependence.Ecol. Monogr., 62 (1992), pp. 277–314.

[19] T. Eavis, A. Lopez, RK-hist: an r-tree based histogram for multi-dimensional selectivity estimation, ACM Int. Conf. on Inf. and Knowl. Management, 2007, pp. 475–484.

[20] Greenwood, P.E., Nikulin, M.S. (1996) A guide to chi-squared testing. Wiley, New York. ISBN 047155779X “Ethics of Information Communication Technology (ICT)”, Regional Meeting on Ethics of Science and Technology, Regional Unit for Social & Human Sciences in Asia and the Pacific, UNESCO, access on 16 Sept. 2011, available at http://www2.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF

[21] Skiena, S. "Lexicographically Ordered Permutations" and "Lexicographically Ordered Subsets." §1.1.1 and 1.5.4 in Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica. Reading, MA: Addison-Wesley, pp. 3-5 and 43-44, 1990.

[22] Charl van der Walt, “Introduction to Security Policies, Part One: An Overview of Policies”, Introduction to Security Policies, Part One: An Overview of Policies, Nov 2010, available at: http://www.symantec.com/connect/articles/introduction-security-policies-part-one-overview-policies

[23] “Data Leakage Worldwide: Common Risks and Mistakes Employees Make”, White Paper, Cisco, 2008 Cisco System, pp. 1-10.

[24] “Technology Roadmap”, Smart Grids, International Energy Agency, Apr. 2011, pp. 1-50.

[25] “Lobby for smart grid roadmap in Malaysia”, Green Purchasing Asia, 2011, available at: http://www.greenpurchasingasia.com/content/lobby-smart-grid-roadmap-malaysia

[26] “Emerging Market Spotlight, South Korea & Taiwan Electronics: Race to the Top”, Thomas White, Mac. 2011, In press: http://www.thomaswhite.com/explore-the-world/emerging-market-spotlight/south-korea-and-taiwan-consumer-electronics.aspx

[27] Phongsak Prasithsangaree, “On a framework for energy-efficient security protocols in wireless networks”, Computer Communications, Volume 27, Issue 17, 1 November 2004, pp.1716–1729.

[28] Yuh-Min Tseng, “A resource-constrained group key agreement protocol for imbalanced wireless networks”, Computers & Security, Volume 26, Issue 4, June 2007, pp. 331-337.