ARPN Journal of Engineering and Applied Sciences >> Call for Papers Vol. 18 No. 7, April 2023

Journal Home

Archive

Submit Paper

Author Guidelines

Editorial Board

Publication Fee

Code of Ethics

Review Process

Upcoming Papers

Contact Us

SJR

ARPN Journal of Engineering and Applied Sciences

Q3 Engineering (miscellaneous)

best quartile

SJR 2021

0.25

powered by scimagojr.com

ARPN Journal of Engineering and Applied Sciences

ARPN Journal of Engineering and Applied Sciences (ISSN 1819-6608) is an online peer-reviewed International research journal aiming at promoting and publishing original high quality research in all disciplines of engineering sciences and technology.

All research articles submitted to ARPN-JEAS should be original in nature, never previously published in any journal or presented in a conference or undergoing such process across the globe. All the submissions will be peer-reviewed by the panel of experts associated with particular field. Submitted papers should meet the internationally accepted criteria and manuscripts should follow the style of the journal for the purpose of both reviewing and editing. Our mission is .....

- In cooperation with our business partners, lower the world-wide cost of research publishing operations.

- Provide an infrastructure that enriches the capacity for research facilitation and communication, among researchers, college and university teachers, students and other related stakeholders.

- Reshape the means for dissemination and management of information and knowledge in ways that enhance opportunities for research and learning and improve access to scholarly resources.

- Expand access to research publishing to the public.

- Ensure high-quality, effective and efficient production and support good research and development activities that meet or exceed the expectations of research community.

Scope of Journal of Engineering and Applied Sciences

- Engineering Mechanics
- Surveying
- Modeling & Simulations
- Manufacturing Technologies
- Metallurgy
- Electronic Communication Systems
- Mining & Minerals
- Applied Sciences
- Chemical Engineering
- Tube Wells & Pumps

- Construction Materials
- Fluid Mechanics & Hydraulics
- Thermodynamics
- Refrigeration & Air-conditioning
- Automatic Control Systems
- Agricultural Machinery & Equipment
- Mechatronics
- Public Health Engineering
- Hydrology
- Structures

JEAS

ARPN

JOURNAL OF ENGINEERING AND APPLIED SCIENCES

Volume 17
Number 23
December 2022
ISSN 2409-5886
e-ISSN 1819-6608

Most Cited Articles (Last 4 Years)

Investigation of Mechanical Properties of PMMA Composite Reinforced with Different Types of Natural Powders (43 Citations)

Smart Healthcare Monitoring System using Raspberry Pi on IoT Platform (99 citations)

The Dynamic Loading Analysis of Containers Placed on a Flat Wagon During Shunting Collisions (42 Citations)

Search

Google Custom Search

Source details

ARPN Journal of Engineering and Applied Sciences

Scopus coverage years: 2009, from 2011 to 2022

Publisher: Asian Research Publishing Network (ARPN)

ISSN: 1819-6608

Subject area: (Engineering: General Engineering)

Source type: Journal

| View all documents > | Set document alert | 🖫 Save to source list | Source Homepage |

CiteScore 2021
1.0   ⓘ

SJR 2021
0.252   ⓘ

SNIP 2021
0.374   ⓘ

CiteScore   CiteScore rank & trend   Scopus content coverage

ⓘ Improved CiteScore methodology   ✕

CiteScore 2021 counts the citations received in 2018-2021 to articles, reviews, conference papers, book chapters and data

papers published in 2018-2021, and divides this by the number of publications published in 2018-2021. Learn more >

CiteScore   2021 ⌄

$$1.0 = \frac{2,634 \text{ Citations } 2018 - 2021}{2,566 \text{ Documents } 2018 - 2021}$$

Calculated on 05 May, 2022

CiteScoreTracker 2022 ⓘ

$$0.9 = \frac{1,750 \text{ Citations to date}}{1,895 \text{ Documents to date}}$$

Last updated on 05 April, 2023 • Updated monthly

CiteScore rank 2021 ⓘ

Category	Rank	Percentile
Engineering		
└ General Engineering	#207/300	31st

View CiteScore methodology >   CiteScore FAQ >   Add CiteScore to your site 🔗

ARPN Journal of Engineering and Applied Sciences >> Call for Papers Vol. 18 No. 7, April 2023

Journal Home

Archive

Submit Paper

Author Guidelines

Editorial Board

Publication Fee

Code of Ethics

Review Process

Contact Us

ARPN Journal of Engineering and Applied Sciences

Editorial Board

Editor-in-Chief: Engr. J. K. Tarakzai   (PAKISTAN)

#	Editors	Country
1	Prof. Dr. R. J. Godwin	UNITED KINGDOM
2	Prof. Dr. Erik Valdemar Cuevas Jimenez	GERMANY
3	Dr. Iftikhar Ahmad	SAUDI ARABIA
4	Prof. Dr. Hamou SADAT	FRANCE
5	Dr. Mohammad Aminul Islam	JAPAN
6	Prof. Dr. Kui Fu Chen	CHINA
7	Dr. Muhammad Imran	AUSTRALIA
8	Prof. Dr. M. Ashraf Chaudhry	NEW ZEALAND
9	Prof. Dr. A. Sermet Anagun	TURKEY
10	Prof. Dr. Ashraf Mohamed Hemeida	SAUDI ARABIA
11	Prof. Dr. Krishna Murari Pandey	INDIA
12	Prof. Dr. Magdy A. Ezzat	EGYPT
13	Prof. Dr. Roberto Brighenti	ITALY
14	Dr. Anurag Misra	INDIA
15	Prof. Dr. Adel M. ALIMI	TUNISIA
16	Prof. Dr. Arun Kumar Gupta	INDIA
17	Prof. Demetrios V. Bandekas	GREECE
18	Prof. Dr. Bensafi Abd-El-Hamid	ALGERIA
19	Dr. Rajanish K. Kamat	INDIA
20	Prof. Dr. Asma Thamir Ibraheem	IRAQ
21	Prof. Dr. Sylejman Hyseni	KOSOVO
22	Prof. Dr. Haider Zaman	SAUDI ARABIA
23	Prof. Dr. Debojyoti Mitra	INDIA
24	Prof. Dr. Pandian VASANT	MALAYSIA
25	Prof. Dr. Prakash MMS Kinthada	INDIA

Associate Editors

#	Editors	Country
1	Dr. Dongning Li	USA
2	Dr. Suheyla Yerel	TURKEY
3	Dr. Guoxiang Liu	USA
4	Dr. Nadeem Anjum	PAKISTAN
5	Engr. Malini Sarah Philip	NORWAY
6	Dr. K.V.L.N. Acharyulu	INDIA
7	Engr. Mohammad Khalily Dermany	IRAN
8	Dr. Lamyaa- Gamal Eldeen Taha	EGYPT
9	Dr. OM Prakash Singh	INDIA
10	Engr. Seyyed Mohammad Reza Farshchi	IRAN
11	Dr. Muhammad Imran Din	PAKISTAN
12	Dr. Jose Carlos Pascoa Marques	PORTUGAL

JEAS

Most Cited Articles (Last 4 Years)

Investigation of Mechanical Properties of PMMA Composite Reinforced with Different Types of Natural Powders (43 Citations)

Smart Healthcare Monitoring System using Raspberry Pi on IoT Platform (99 citations)

The Dynamic Loading Analysis of Containers Placed on a Flat Wagon During Shunting Collisions (42 Citations)

Search

Custom Search

13	Engr. Fawwaz Jinan Jibrael Jabri	IRAQ
14	Dr. Kanad Ray	INDIA
15	Dr. Shamsuddin Shahid	MALAYSIA
16	Engr. Naveenji Arun	INDIA

Search

Google Custom Search

Home

Archive

Submit Paper

Author Guidelines

Editorial Board

Publication Fee

Title: Perfect shuffle algorithm for cryptography

Author (s):   Ernastuti

Abstract: The problem of protecting the messages from the hackers is usually solved by cryptographic methods. This led to create various algorithms of encryption and decryption. This paper proposes the new algorithm based on perfect shuffle technique. It is called Perfect Shuffle Crypto Algorithm (PSCA) which is classified as a transposition or permutation technique in the crypto system. The PSCA is an asymmetry key encryption, uses a pair of keys, that are a public key for encrypting data, and a corresponding private secret key for decrypting. PSCA is very fast and simple for technical realization. For the linear plaintext length of $N=2^n$, it will take O (N log N) to complete both encrypting plaintext and decrypting cipher text. The PSCA is reasonably secure, especially for chipertext-only attack. It is enable to apply PSCA as an basic algorithm alternative to develop or create an crypto algorithm which employ the layered scheme.

Full Text

Title: Combinatorial gray code for generating tree of permutation with two cycles

Author (s):   Sulistyo Puspitodjati, Henny Widowati, Asep Juarna and Djati Kerami

Abstract: Combinatorial Gray Code is a listing of all considered combinatorial objects so that every two successive objects differ in some pre-specified way. This paper concerns of a combinatorial class namely permutations with two cycles. In our research these permutations have been developed using generating tree. The generating tree is then coded, and listing the node of this tree will be shoed as a Gray code. In this paper we proposed a new combinatorial Gray code. We give the construction of the Gray code for this coded generating tree of generating permutation with two cycles. The Gray code will be measured by its Hamming distance in order to show that it is a Gray code.

Full Text

Title: Discovering sequential disease patterns in medical databases using freespan mining and prefikspan mining approach

Author (s):   Silvia Rostianingsih, Gregorius Satia Budhi and Leonita Kumalasari Theresia

Abstract: Dr. Soetomo General Hospital had computerized their system to stored inpatient's history. With lots of data to be analysis, one of the needs is a decision support system in order to anticipate the spread of the disease. Therefore the hospital need a system to provide the sequential pattern of disease. One of the sequential pattern mining algorithm is pattern growth based approach. The result is sequential pattern of disease from particular area in a time period based on inpatient's history. Input from user are time period, minimum support, province, and multi-dimensional. The system built with Java Net Beans 6.7 and Oracle 10g. This research showed that FreeSpan and PrefikSpan produce the same output. However, FreeSpan is more appropriate for dr. Soetomo General Hospital because the proccesing time is faster.

Full Text

Title: Heroic battle of Surabaya application based on android

Author (s):   Andreas Handojo, Justinus Andjarwirawan, Sandy Sunaryo and Resmana Lim

Abstract: The limitation of teaching media that using current method such as book, white board, etc. now have a new problem to get student attention and interest to learn. Meanwhile, within the progress of electronic technology especially mobile device, enhanced access to any information for everyone. Therefore, in this research we like to integrated mobile based learning that cover any learner style (visual auditory kinaesthetic) so can improve student attention and interest to learn. This mobile based learning application will dedicated for learn nation history, especially heroic battle 10 November 1945 in Surabaya. This application will give the information such as battle history, battle historical location information include location photo gallery and tagging information on a Google Map, video, sound, and quiz, to provide a thorough understanding of fascinating history from the events surrounding the battle. And to improve learning process for student and also for more interesting, this application also provides Global Positioning System (GPS) connection to get position of the user and using it to get

direction to historical location using Google Map. This application will provide a list of locations that have been visited by the user (by GPS detector) that also unlocked a new feature of this application, so user not only read about the historic sites but also can explore all the historic sites in Surabaya and found fascinating city of Surabaya. For improvement, we proposed a way to download and update content using zip file technology so user not need to upgrade entire application to add content. This result from this research will evaluate using questionnaire to 200 respondents with a variety of ages and educational backgrounds, to found the user opinion about this application.

Title: Analysis of the impact of information technology investments-a survey of Indonesian universities

Author (s):   Leo Willyanto Santoso and Yulia

Abstract: In recent years, the utilization of information technology has been magnificently increased in service industries, particularly, education institution, which by using Information Technology related products such as academic information system and learning management system. In Indonesia, universities invest enormous resources in information technology (IT), with little evidence of the latter's effectiveness. Stakeholders struggle with gauging how effective or ineffective making these investments truly is, given the lack of instruments of measurement by which to establish, for instance, an internal rate of return or a period of recovery on investments. This paper investigates the impact of investment in information technology on the return on assets (ROA) of selected private universities in Indonesia for the period 2008 - 2014 using Adapted Information Economics. By using this method, it is possible to implement into other university. Primary and secondary data were collected during this research. The study recommends that universities should increase investments in software, hardware and infrastructure which will enhance their Management Information System and profitability.

Title: Interactive game design for learning of united nusantara in the majapahit era

Author (s):   Liliana, Erandaru, Gregorius Satia Budhi and Silvia Rostianingsih

Abstract: Know the national history is important to develop patriotism. Nowaday, young generations have less interest on learning national history. It needs creative media to deliver the content of history to them. If history is packed as film, picture book, animation or a popular media lately, computer game, it will be easier to be learn. Observing the need to introduce Indonesian National history especially to young generation, in this research will be developed a learning scheme through an interesting media, computer game. In designing game which adopt some important aspects in history, game play and story board plays a significant role. This game will contain three aspects socio-cultural, government and economy. These aspects are selected because represents modern Indonesia's condition. They are diverse ethnic groups, archipelago country and similar economic as living support. Socio-cultural aspect will be represented by daily activities and public buildings. Governmental aspect will be represent by arrange territory and military. Economy aspect will show agriculture, trading and mining. This game is a strategy turn based game because the main goal of this game is to unity the entire island in nusantara (Indonesia). Since every player can make different strategy, this game can yield different results. This situation limits delivering history content. Socio-cultural, governmental and economy aspect are not depend on chronology. Thus, these aspects can be represented in the game appropriately. To limit the wide area of nusantara and the long history since the first king of Majapahit until the last king, this game is limited until entire nusantara island are conquered. This time is about King Hayam Wuruk era.

Title: Implementation of wireless mobile sensor based on fuzzy logic control for LPG GAS pipeline leakage monitoring

Author (s):   Riny Sulistyowati and Kunto Aji

Abstract: The main purpose of the leakage detection system on a gas pipeline is to give a warning of the dangers related to a gas leak that could endanger human lives and cause material loss. There is a wide range of gas detection systems used to provide an early detection and warning in the event of a leak in a gas pipeline, one of which that is wired monitoring system. However, in its implementation, the wired-based monitoring system has many shortcomings. To overcome the disadvantages of the wired monitoring system, a wireless-based sensor network in detecting and monitoring gas pipelines is applied in this study by implementing mobile sensors as key components of the data collection. LPG mobile sensors used in this study are equipped with a pipe tracking algorithm based on fuzzy logic control algorithm, so they can easily track and monitor the installation of a gas pipeline. Fuzzy logic control achieves a success rate of 70%. The overall system testing results in the average error of 18.5%, indicating that the mobile wireless sensors can already detect leakage in LPG gas pipelines.

Title: Vapor identification system using Quartz resonator sensor array and support vector machine

Author (s):   Hari Agus Sujono and Muhammad Rivai

Abstract: It has been developed a vapor identification system using gas sensor array and Support Vector Machine (SVM) pattern recognition. Sensor array consists of several quartz resonator sensors coated with different polymer materials in order to have a specific pattern to the vapor. In this study, the Field Programmable Gate Array was used as counters and other functions to interface the sensor array with a computer. Frequency change was measured by a counter with a period of one second. Vapors used in the experiment were kerosene, methanol, gasoline and alcohol. The data analysis was taken from the frequency changes after vapor injection. Sensors were cleaned to get the initial condition using nitrogen gas. For vapor data collecting, the measurements were performed eight times for each sample. The set of digital data was then stored as a database. Principle Component Analysis was used to visualize the performance of the sensor array to discriminate each vapor. The set of vapor pattern obtained by the sensor array was then identified by SVM algorithm. Experiment results showed that the

SVM could identify each vapor with a success rate of 97.2%. The results of this study will be used for further research to detect the low concentrations of vapors contained in human breath for medical diagnoses.

Full Text

Title: Internet-based applications to help design security system in the organization

Author (s): Agustinus Noertjahyana, Ibnu Gunawan and David Lawrence Kusuma

Abstract: This paper presents the results of research related to the development of the design of security systems in an organization. So many functions of management is done with the help of the internet. However, there is still many IT staff in organizations that do not pay attention to an important aspect of security. So that the IT staff is still focused on the development of applications that support operations, but have not thought about the need for a security system. IT staff are just beginning to realize how important the security system for the application when it attacks both from outside and within the organization. IT staff often do not know where to start to make a security system design. For those reasons, research on how to design a security system becomes a necessity for organizational IT staff to be able to take precautions against an attack that will appear later. The purpose of this research is to help IT staff to be able to design a security system from the planning phase, implementation phase, and phase control. This study uses a framework based on the 10 CISSP domains that will be implemented in an application. By applying CISSP framework into the application, the expected results of this research are useful to assist organizations in determining security priorities, the results are in the form of an application that contains the planning, implementation, and monitoring of any design project security system in the organization.

Full Text

Title: Open protocol framework for telepresence robot

Author (s): Petrus Santoso and Handry Khoswanto

Abstract: Research on telepresence robot has a lot of unexplored potential. Many researches have been done to pursue development on telepresence robot. Most of the researchers usually buy a commercial telepresence robot or build a special purpose one. Usually the needed protocol is developed from scratch. The developed system seldom has interoperability between each other and the process can be costly or lengthy. To expedite research process on telepresence robot development, this paper tries to present an open protocol framework for telepresence robot. The framework will consist of architecture definition, service specification and protocol specification. An implementation of open protocol framework has been simulated. A working hardware prototype that implemented the framework also has been built and tested. The result shows that the open protocol framework is useful and easy to implement. All the implemented protocol functions working properly. The function call of the SPs can be configured according to the needed parameters.

Full Text

Title: Pakar-ukm - expert system for smes using dynamic knowledge base

Author (s): Mohammad Iqbal, Sigit Widiyanto, Haydan Mardhi Fadlillah and Herry Susanto

Abstract: The rapid developments in the field of Information and Communication Technology (ICT) opens wide opportunities for Small Medium Enterprises (SMEs) in Indonesia to be able improving its performance in producing, marketing and even to conduct business planning by analyzing patterns of every days business transactions. Additionally, ICT costs in Indonesia are getting cheaper, and the changes of SMEs activist perception that ICT can be improve the performance of their business had increase the value of their confidence towards more intensive the adoption of ICT in their works. However, the adoption of ICT process is still experiencing obstacles such as a lack of expertise and skill in producing or managing advanced technology in line with business needs. One solution is the assistance offered by the ICT practicing, to get a optimal solution, So the ICT is not only used for business operational purposes only, but furthermore can be used as business Intelligence function for SME business development planning. This study was a meta-analysis of the behavior patterns the adoption of ICT by SMEs in Indonesia from individual studies that have been done before. Based-on that study, we designing a business intelligence system that best suits to the characteristics of SMEs business behavior were found. In general, the expert system can be use as the most suitable method for SMEs in Indonesia, and in this study, we have accomplished developing a prototype of expert system with a dynamic knowledge based using data mining by doing a classification and web crawling to generate high quality results to accommodate decision making for small and medium enterprises..

Full Text

Title: A low power low noise COMS amplifier for portable ECG monitoring application

Author (s): Jun Giap Lau and Arjuna bin Marzuki

Abstract: A low power and low noise front end chopped instrumentation amplifier for portable electrocardiogram recording system is presented. The circuit is based on the chopper technique which is implemented using folded cascode structure that has significant lower power consumption than the predecessor's approaches while keeping the performance unchanged. The chopper switches modulate noise from a low frequency into a higher frequency range, then demodulates back to original signal before filtering the unwanted effect by a low pass filter. The circuit is designed based on SILTERRA 0.18 μm CMOS technology process using VIRTUOSO CADENCE. The simulated results of the amplifier show ultra-low power of 5.51 μW and low noise of 17.2 μV/√Hz at 10 Hz. High differential voltage gain of 54.5 dB and 71 dB in CMRR are achieved.

Full Text

Title: A nurse following robot with high speed kinect sensor

www.arpnjournals.com

INTERNET-BASED APPLICATIONS TO HELP DESIGN SECURITY SYSTEM IN THE ORGANIZATION

Agustinus Noertjahyana, Ibnu Gunawan and David Lawrence Kusuma
Siwalankerto 121-131, Surabaya, Indonesia
E-Mail: agust@petra.ac.id

ABSTRACT

This paper presents the results of research related to the development of the design of security systems in an organization. So many functions of management is done with the help of the internet. However, there is still many IT staff in organizations that do not pay attention to an important aspect of security. So that the IT staff is still focused on the development of applications that support operations, but have not thought about the need for a security system. IT staff are just beginning to realize how important the security system for the application when it attacks both from outside and within the organization. IT staff often do not know where to start to make a security system design. For those reasons, research on how to design a security system becomes a necessity for organizational IT staff to be able to take precautions against an attack that will appear later. The purpose of this research is to help IT staff to be able to design a security system from the planning phase, implementation phase, and phase control. This study uses a framework based on the 10 CISSP domains that will be implemented in an application. By applying CISSP framework into the application, the expected results of this research are useful to assist organizations in determining security priorities, the results are in the form of an application that contains the planning, implementation, and monitoring of any design project security system in the organization.

Keyword: CISSP, internet-based applications, security design.

BACKGROUND

In the operations of organizations that use information technology based on computer networks, it is necessary to take into account the security of data in information systems. Security has become one of the important factors in the sustainability of the organization's activities. The more complex the organization using information technology, the security system will become more important [1].

Common problems associated with security systems for examples: computer or laptop thefts, theft of data due to transmission lines that are less secure, data centers are not secure because there is no access control, no security policy in the organization, the data can be easily read by unauthorized, natural disasters, the development of applications that do not use the principle of security, and operational activities of the organization are not concerned with the security aspect.

Many organizations invest heavily to protect the existing system. However, problems often arise on how to do the planning, operational until the stage of evaluation of existing security systems.

Problems that arise are the IT staff often find it difficult to make a good security system design, ranging from planning, implementation to evaluation stage. Very rarely organizational policies related to the design of security systems. For that it is necessary to develop an application that able to map CISSP framework into a system, which is useful to overcome these problems.

This system will help IT staff in the planning of the security system, so that the IT staff is able to make the design of security systems within the organization from the planning phase, the operational phase and evaluation phase.

The expected result is the existence of a system that is able to provide support at the management level to determine what steps will be taken to improve the security system in the organization.

SECURITY PRINCIPLES

The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [2].

Information security must be supported by a reliable security system, because it has the goals:
Integrity - ensuring that the data has not changed and no damage.

Confidentiality - ensuring that the data is confidential so that the information can not be seen by unauthorized.
Availability - ensuring that information is accessible whenever needed.

Each organization has different priorities in determining the security used. Government, military, corporations, financial institutions, and hospitals focus on confidential information about their customers, financial status, products, and research [3].

Companies that focus on electronic commerce, the main focus on availability, so that when the system is down, will cause a loss for the company both financially and reputation.

Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers [3].
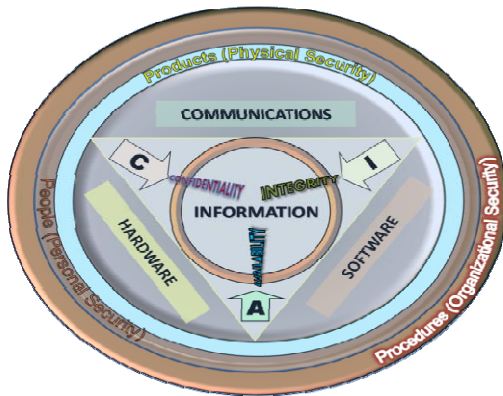
www.arpnjournals.com

Figure-1. Relationship of Confidentiality, Integrity and availability.

SECURITY POLICY

Security policy is a plan that describes the important assets of the organization, and how to protect it [1]. The purpose of the Security policy is explain to the user what the assets are permitted and are not allowed to access. Documents must be clearly understood by the user in order to be able to understand the potential targets in the security system.

Security policy must meet the following requirements:

a) How sensitive information secured.
b) How to maintain username and password of each user.
c) How is the response to security incidents?
d) How to use a computer and internet connection securely.
e) How organizations use email correctly.

The procedure how to run a security policy is the security policy and what to do in case of violation of the security policy.

Here are some of the items included in the IT security policy:
1. Policies for the end user
   - The use of CD-ROMs and flash
   - Passwords
   - Backup Files
2. Policies for the Department
   - workplace safety procedures
   - Alarms
   - Knowledge of information systems
3. Policies for System Administrators
   - Procurement of hardware
   - Access Control
   - Computer Networks
   - Operating system (OS)
   - Software
   - Cyber crime

   - Backup Database
   - Local Area Network
   - Protection against viruses
4. Policies for Database Administrators
   - Transfer Procedure and data changes
   - Data Storage
   - Databases

INFORMATION SECURITY AWARENESS

Employees' information security awareness is an important part of an effective information security management program [4]. For the organization, the higher the level of staff awareness of the organization's security system, the security level of the organization will be higher.

CISSP

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the International Information Systems Security Certification Consortium, also known as (ISC) ².

Technological solutions alone cannot protect an organization's critical information assets. Employers demanding qualified information security staff give their organizations a leading edge by providing the highest standard of security for their customers', employees', stakeholders' and organizational information assets. (ISC)², the only not-for-profit body charged with maintaining, administering and certifying information security professionals via the compendium of industry best practices, the (ISC)² CBK®, is the premier resource for information security professionals worldwide [5].

CISSP certification helps companies to identify individuals who have the ability, knowledge, and experience necessary to implement good security practices, perform risk analysis, determine the necessary countermeasures, and helps organizations to protect facilities, networks, and information.

CISSP divides the definition of security in the 10 domains, as follows [6]:

a) Information Security Governance and Risk Management

Professional in the field of information security is capable of evaluating the risks of the organization's critical assets and use security systems to mitigate them. Many types of jobs such as firewall engineers, penetration testers and auditors have different risk and impact for any organization depends on the structure and needs of each organization.

Domain Information Security Governance and Risk Management focuses on risk analysis and mitigation of risks, which include security governance, or organizational structures needed for the success of information security programs. The difference between a successful organization and the failure is not related to

money and the number of staff, but using the right people in the right positions.

b) Access control

Domain Access Control focus on protection against unauthorized access, modification of data, and loss of confidentiality. Access Control can be achieved by applying the technique, physical, and strong administrative measure.

In Access Control, not only the term confidentiality, integrity and availability should be considered, but should consider of identification and authentication, authorization, and accountability [7].

Identification and authentication is required to prove that only the identity of the person who could legitimately have access to the system. Identity is weak because there is no evidence, and others can serve as a legitimate person to get into the system.

To prove that the only legitimate person who can get into the system, it would require an authentication process, which can be done by showing information such as a password or passport. Authorization describes the actions that can be performed by the system after passing through the phase of identification and authentication. This can be done with read, write, and execute files or programs.

Accountability keep users accountable for the actions that have been performed. This is usually done by analyzing the data logging and auditing. For some users, knowing that the data has been recorded is not enough to stated its responsibility but should be recorded and re-calibration at each specific time period.

c) Cryptography

Cryptography domain focuses on protection of confidentiality of information. Cryptography is a means to make a communication to be safe, because the information sent can only be understood by the sender and the recipient.

The purpose of cryptography is to provide protection if the information had been stolen by an unauthorized person, but can't get the information because the information is encrypted.

Encryption is a method of changing the data that can be read, called plain text, into a form that is random and can't be read, called cipher text. Plain text is a form that can be read by humans (documents) or engine (executable code), but once converted into cipher text, it can't be read by humans or machines. To be able to read the plaintext, it is necessary to process the decryption of the cipher text. This allows the transmission of confidential information over insecure channels.

d) Physical (Environmental) Security

Domain Physical (Environmental) Security focuses on the protection of the confidentiality, integrity, and availability of physical assets such as people, buildings, systems, and data. CISSP considers human safety as the most important concern in this domain.

Domain Security perimeter helps prevent, detect, and correct physical access unauthorized entry. A building must use a layered defense. Important asset to be protected by physical security such as fences, doors, walls, locks, and so on.

e) Security Architecture and Design

Domain Security Architecture and Design focuses on the explanation of the logic, hardware, operating systems, and software security components and how to use it for designing and evaluating secure computer systems.

f) Business Continuity and Disaster Recovery Plan

Domain Business Continuity Planning and Disaster Recovery Planning (BCP / DRP) focuses on prevention against events such as illness, loss of life, natural disasters and the failure of the organization. Disaster is an inescapable fact of life. Referring to the threat of an event and a possible threat occurs, should be prevented / reduced by appropriate measures in the organization.

The purpose of BCP is to ensure that the business will continue to take place before, during, and after disasters, by providing long-term business strategy after the disturbing events occur.

Disaster Recovery Planning (DRP) provides short-term plan to disturbances arising, and typically relate to IT. DRP focuses on efficiency to reduce the impact of disasters and immediate response and recovery of critical IT systems. It is considered to be tactical rather than strategic because it provides a means to quickly respond to the disturbance.

g) Telecommunication and Network Security

Telecommunications and Network Security domain focus on the description of the design and architecture and secure communications network. This includes the selection of the appropriate network devices, the use of firewalls and Virtual Private Network.

h) Application Development Security

Domain Application Development Security focus on how to develop software correctly and securely. Software is everywhere, not only in computers, but in the home, car, and medical equipment. More complex the software, more errors that can occur. Developing reliable and secure software is very important. It can be started from the concept of good programming, the selection of appropriate methods of application development, testing and looking for software vulnerabilities.

i) Operations Security

Domain Security Operations focus on the threat to the production environment. Threats can come from internal or external to the organization. Internal threats often arise from employees who are not satisfied with the organization. Operations Security includes administrative security, Media Security, Continuity of Operations.

www.arpnjournals.com

Administrative security provides ways to control access to operational data. Some aspects to consider are: Separation of Duties, Job Rotation, nondisclosure agreement, Background Checking, and Change Management.

Media Security about the process of handling the security of the media used by the organization. Some aspects to consider are: Storage and Media Sanitization or Destruction of data.

Continuity of Operations about the process of to ensure that the activities of the organization should continue under any circumstances. This can be done by a Service Level Agreement with outsiders, and fault tolerance on the design concept of each equipment.

j) Legal, Regulation, Investigation, dan Compliance

Domain Legal, Regulations, Investigation, and Compliance focus on some basic legal concepts that are important for all professionals in the field of information security, including intellectual property, and violation of privacy, but in some parts of the world, this concept is universal.

DESIGN AND IMPLEMENTATION

The design process of this research refers to the CISSP. Stages of implementation of this security system design are:

a) Choose Project

At this stage the administrator could choose an existing project or create a new project. The initial process will show 3 menu are: About, Projects, and the Choose Project. 'About Menu' featuring Team Software Developers 'Projects Menu' displays existing projects and Administrators can create new projects, and 'Choose Project' featuring a selection of existing projects. Design menu on the main page can be seen in Figure-2.

Figure-2. Home Menu.

After selecting the menu 'Project', it will display a list of projects that have been, or could choose to add the new project. An existing project can be renamed or deleted. The new project can be added by selecting the 'Add Project'. Menu 'Project' can be seen in Figure-3.

Figure-3. List of Existing Projects.

Selection of projects can be done by selecting the menu 'Choose Project', and will display the sub-menu option that can be seen in Figure-4. If the selected Project is a new project, the 'Operational', 'questionnaire', and 'Result' can't be selected before the Planning process is executed. This is an additional feature that can help the administrator to make the design process appropriate with the existing order.

Figure-4. Sub-Menu Choose Project.

b) Planning Process

This section helps administrators to plan for the needs of the system with reference to the CISSP standard. Each domain has given some standard so that the administrator can choose which suit the needs of the organization. Additional standards can be given by the Administrator if the organization requires one or more standards and yet in each domain, but still should be in the 10 CISSP domains.

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

Figure-5. Display of Planning Process.

In Figure-5 displays the first domain: Information Security Governance and Risk Management. There are 13 standards in accordance with the standards of the CISSP but if the administrator wants to add another standard, can be done by pressing the '+' and the display will look like in Figure-6.

Figure-6. Adding Standard for Each Domain.

c) Operational Process

This section helps administrators by providing the risk of each chosen CISSP standards. Administrators can choose the best plan of each standard selected in accordance with the system. This section will display the risk of each item that not be chosen. After completely checking the standards needed, administrators can generate the questionnaire or print the checklist of the operations.   The process can be recorded each period. Period used is monthly, so that the administrator can perform checks every month. Operational Process in

the Domain Security Architecture and Design is shown in Figure-7. In the Domain Security Architecture and Design only selected 3 standards, and for standards that are not selected will be shown the risks of each standard.

Figure-7. Domain Security Architecture and Design.

d) Create a questionnaire

Menu 'Questionnaire' can be generated after the administrators choose the standard that exists in each domain. The objective of this questionnaire is to assist the Administrator in getting feedback on any questions related to the standards that exist in each domain. Once the questionnaire is formed, then the administrator can pick the type of questions to be given to the user to get feedback based on each domain. Form questionnaire can be seen in Figure-8.

Figure-8. Sample of Questionnaire.

e) Report

This section displays the results of the Risk Assessment of the selected project. Each standard grouped in each domain and sort by priority domains. Domains that have a higher priority, which means it has a greater risk. Each standard is given a color that corresponds to the level of vulnerability. Dark green color means the risk is very low. Green means low risk. Yellow means moderate risk. Orange means a high risk. Red means the risk is very high. The results of the application can be seen in Figure-9.
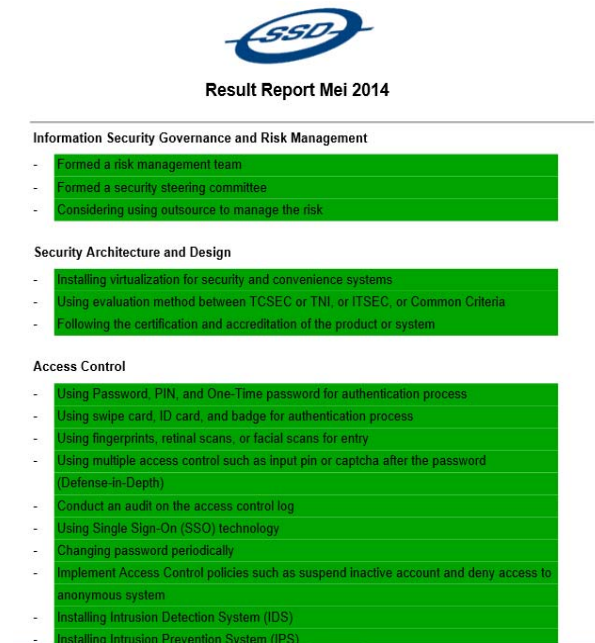

Figure-9. Result of Application.

CONCLUSIONS

CISSP can help to map the inside of the security system by dividing into 10 domains. Each domain has its own standards and is flexible, so that each domain can also be customized according to the needs. By doing a good security system design, from the planning phase, the operational phase, until the evaluation stage, can help IT staff to create a security system that suits the needs of the organization, also improve staff's security awareness.

REFERENCES

[1] Ibnu Gunawan, Agustinus Noertjahyana, Hartanto Rusli. 2014. Analysis and Implementation of Operational Security Management on Computer Center at the University X. Conference, Competition and Exhibition. pp. 888-896.

[2] U.S. Code collection http://www.law.cornell.edu/ uscode/44/3542.html.

[3] Sattarova Feruza Y. and Prof. Tao-hoon Kim. 2007. IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering. 2(2): 17-31.

[4] Burcu Bulgurcu, Hasan Cavusoglu, Izak Benbasat. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and information Security Awareness. Bulgurcu et al. /Information Security Policy Compliance, MIS Quarterly. 34(3): 523-548.

[5] CISSP - Why Certify https://www.isc2.org/cissp-why-certify/default.aspx.

[6] Eric Conrad. 2011. Eleventh Hour CISSP Study Guide. Amsterdam. Elsevier.

[7] Shon Harris. 2013. All-in-One CISSP Exam Guide. Sixth Edition. New York : McGraw-hill Companies.