Foreword and Editorial

International Journal of Reliable Information and Assurance

We are very happy to publish this issue of an International Journal of Reliable Information and Assurance by Global Vision Press.

This issue contains 5 articles. Achieving such a high quality of papers would have been impossible without the huge work that was undertaken by the Editorial Board members and External Reviewers. We take this opportunity to thank them for their great support and cooperation.

In the research "A Methodology for Assessing Security Vulnerability of Cloud Services", cloud services continue to change the business paradigm to use computing resources such as infrastructure, platform and application using the network access. They have created new security threats and challenges. When large amounts of data are saved in the cloud, the cloud is naturally exposed to attack. In cloud services, analysis and evaluation of security vulnerability should be made with protection plans that provide the objective data and information necessary to establish measures for information protection for each business of firms and take into account the impact on their respective responsibilities. This paper presents a framework to evaluate security vulnerability that reflects the business impacts. Through this framework, it is possible to evaluate vulnerability items of cloud services. Eventually, the proposed methodology will help establish security policies for both cloud service providers and users.

In the paper "Using IDoT Attributes for Secure Power Data Sharing Based on Blockchain Dynamic Access Control", data collected through devices are stored in a single cloud and processed in Internet of Things (IoT) environment. Because IoT has a limitation of computing and storage space of devices. In order to solve the problem of reliability of centralized system, previous researches have been carried out to link blockchain to the Internet. However, user privacy protection is an indispensable factor for sharing data through the Internet. However, these limitations are not overcome. In this paper, the access control of the user is made flexible and robust through Dynamic Access Control Table (DACT) using the context attribute of IDentity of Things (IDoT). The system proposed in this paper can build a platform to securely share users' power consumption data in the energy cloud.

In the survey paper "A Survey on Essential Strategies for Avoiding Cloud Data Leaks", as of late, there has been a tremendous development from putting away information the customary route, as the cloud has developed and turned into the better answer and alternative for organizations and associations alike. Notwithstanding, this has additionally prompted a development in digital culprits and information breaks now that somebody can get to touchy archives from their lounge room love seat. In that capacity, cloud information spills have turned into a very regular issue for organizations. More news has examined approaches to counteract breaks, and you can discover a plenty of articles that discussion about huge and little organizations alike being assaulted. Therefore, knowing how to keep a cloud information spill is the initial phase in protecting your business and data. In this paper there are a couple of the best and most straightforward methodologies to maintain a strategic distance from cloud information spills.

The paper entitled “Implementation of Low Cost Memory Subsystem for Low-end IoT Devices” explored that the increasingly popular IoT devices and cloud computing devices are being developed in various models from high to low price, but the low-cost market is still growing more actively. In these devices, where internet communication is a key feature, the most expensive components are memory and screen panels. Currently, screen panels are limited in LCD and OLED technology, so the choice is small, but memory includes flash memory, hard disk, DRAM, SRAM, SDRAM, multi-bank memory, and on-chip memory. Therefore, each type is selected and configured according to requirements such as function, power consumption, performance, and cost. The choice of memory architecture available for low-cost IoT devices is quite limited, with a small configuration of SRAM and some flash memory or DRAM. In the case of hard real-time IoT devices, it is very difficult to meet the deadlines in such a memory structure, and developers apply various system optimizations to solve them. Normally, multibank DRAM is selected at the hardware design stage. Parallel access to as many bank memories as possible in the same space can significantly improve system performance. If the hardware is selected as multi-bank memory, there must be system software to support it. In other words, a compiler must be provided to generate program code for parallel memory access. This is because traditional compilers generate program code for sequential access. In this paper, we propose a parallel memory access program code generation method for multi-bank memory support of low-cost IoT devices. The proposed method solves the data placement problem for multi-bank memory and maximizes system performance by actively using multi-bank memory.

In the review “A Detailed Review on Focus Areas of Cyber Security”, security is one of the most important factor or point to be considered for everyone in their life. Providing security and breaking the security are two important points to be noted for everyone who can be using the gadgets in these days. The other important factor or the point to be considered was the cyber security. The attacks or the collection go data unethically without the knowledge of the user’s being stolen. The cases or the issues being under this trap are being increasing from time to time and day to day in those days. The data to be stolen will be used for various reasons. Some may be using for money collection and some are using it for anti social elements and unethical issues. Hence, in the current article an attempt has been made to provide a detailed idea of the types of attacks and types of issues and types of malwares that can be attacked and also some suggestions were provided. The important issues to be focused in the case of cyber security issues are given a thought and the details are given a light on it. The readers of this article can get the basic knowledge about the cyber security issues and threats and the steps to be followed such that to escape from these sorts of attacks. Also a focus was given on various aspects such that to escape from these types of security attacks.

December 2019

Dongho Won, *Sungkyunkwan University, Republic of Korea*

Editor(s)-in-chief of the December Issue on
International Journal of Reliable Information and Assurance