Chapter 18
Security Threats and Solutions for Virtualization and Migration in Virtual Machines

N. Ravi and N. R. Sunitha

Abstract Cloud has been a dominant player in information technology in the recent years. The main composing factor of cloud is virtualization among many others. Due to the widespread acceptance of cloud, the researchers have identified that the area is a favorable habitat for the attacks. The attacks and threats always have poured gloomy clouds on the user raising the concern about their privacy and security. The virtualization technology dates back to the advent of mainframe computers and has been the area of refinement over the years. Since the cloud is built on obsolete virtualization technology, it eases the combination of attack pattern for the malicious user. Also, the migration of virtual machine (VM) holds key status in the effective management of data centers. As the virtualization technology imbibed on cloud is obsolete, the migration technique is also prone to attack and ineffective management. This paper discusses the threats and associated attacks pertaining to virtualization and migration in VM and proposes a new framework which will enhance the security of virtualized environment. The proposed framework handles the migration of VM in an effective manner.

Keywords Virtualization · Virtual Machine (VM) · DASDVM · Security threats · Migration · Cloud computing threats · SLA

18.1 Introduction

Cloud computing or simply cloud refers to the technical setup of hardware resources and software implementation which makes realization of several crucial business requirements such as availability, performance, security, scalability, accessibility, etc., to run a business effectively. The kind of freedom of operation was facilitated for the cloud by the advent of new technologies such as virtualization, service-

N. Ravi (✉) · N. R. Sunitha
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, Karnataka, India

N. S. V. Rao et al. (eds.), *Proceedings of International Symposium on Sensor Networks, Systems and Security*, https://doi.org/10.1007/978-3-319-75683-7_18

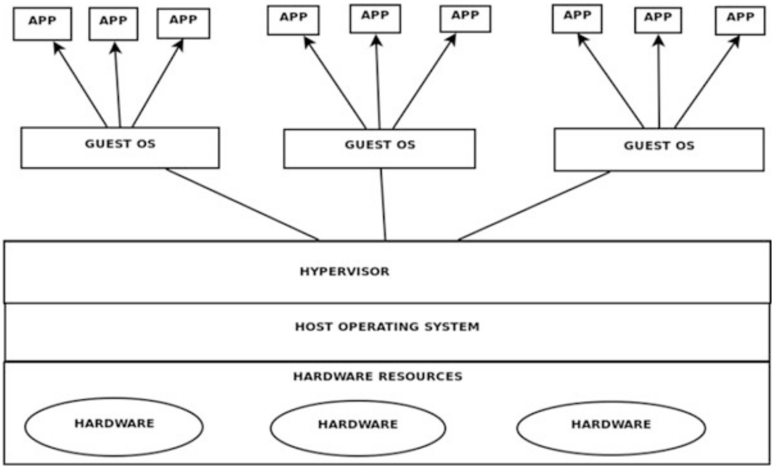

Fig. 18.1 Hosted virtualization

oriented architecture, automatic computing, and web services, among others. Virtualization is a remarkable and noteworthy technology that separates physical resources and creates an illusion of dedicated resources of the hardware/software which will cater to the needs of the user. This is done with the help of hardware, software, or combination of both. A virtual machine monitor(VMM)/hypervisor is a piece of software or hardware that instantiates the virtual instances that the VM emulates a guest operating system (OS) and presents a distinct instance of the host operating system to mimic the fully functional OS. The VMM is an intermediate component and a lightweight module implemented either by software or hardware [4]. This is illustrated in Fig. 18.1. Based on the type of implementation, virtualization can be broadly of the following breed, namely, hardware virtualization and software virtualization. Virtualization can also be done on several layers such as hardware, software, memory, data, network, and storage.

18.2 Security Issues and Categorization

Although, the virtualization has paved the way for the tremendous ascendancy of cloud computing, industry experts and researchers put forth the view of concerns for the security [8]. The security definition has evolved over the years considering the scale, usage, context, and other several parameters. The transition has been from an amoebic fringe to layered multidimensional scale. Traditionally security was coined around the terms integrity, confidentiality, and availability. These revolved around and referred to data in general. Today's Internet has grown beyond data without losing the centrality to data. Concerns that are originating and prevailing in recent times lie in layers such as architectural issues, network issues, and legal issues. Among the security issues, we concentrate on virtualization mainly because of the minimal work done on the particular domain of virtualization and as it is one of the building blocks and major contributing factor which is binding the cloud architecture today. We can identify the security issues such as VM image splitting, VM isolation, VM sprawl, VM rollback, VM escape, VM migration, hypervisor issues, cross-VM side-channel attack, VM creation attack, and VM scheduler attack [1, 7, 9] and more on the virtualization front. The acquaintance of each of the concerns is as follows.

VM image splitting: A VM image repository is used to fire up the process of instantiation. A VM image repository could be used by malicious user to access the VM image and do changes which could potentially harm the repository base and also can compromise the multi-tenant environment.

VM isolation: A VM needs to be isolated from one another in order to create a safe multi-tenant environment. Although the VMs are logically differentiated, they access the same underlying hardware resource.

VM sprawl: It is a condition wherein a number of VMs are instantiated on the host which are growing exponentially, and most of them are either underutilized or idle which does not serve any purpose. This leads to poor resource utilization.

VM rollback: Rollback is a technique where the VM can be reverted back to the last known good state. This can be done with the help of log files. This helps the VM in case the migration process fails. The rollback provides the user the freedom and resilience. On the other hand, this process can revert back the privacy and configuration settings that were previously disabled.

VM escape: It is a condition where the VM escapes or gets abducted from the control of hypervisor or VMM. This condition affects the underlying hardware resource and makes the hardware resources available to the malicious user; the user can do demonic acts with the access to the resource. The IaaS model is the most affected model with this condition.

Hypervisor issues: The influential piece of software that manages the VM is the hypervisor or VMM. It beholds the duty of orchestrating the process of virtual resource allocation and management. If this module is compromised, then there are endless possibilities for the intruder to carry out. The intruder always looks for the loopholes of the VMM or the weak entry point to gain access to VMM.

Cross-VM side-channel attack: This condition can occur in the VMs dwelling on the same physical host as that of attacker where in the information such as keys, resource spending is being exposed and stolen by the attacker.

VM creation attack: A malevolent code could be placed inside the VM image before the instantiation process; thereby when the VM creation process outsets, the resultant VM is an outcast.

VM scheduler attack: Loopholes in scheduler can result in theft of service or resource abduction. For example, the VM's scheduler is scheduled to run at a particular instance preserving the credit balance of the time slice.

VM migration: This is a mechanism of transferring the VM from one physical host to another without shutting the VM down. Summarizing the security threats pertaining to the virtualization layer, all the abovementioned pitfalls raise the concern in a substantial way.

18.2.1 Migration of VM

This is the process of transferring the VM from one host machine to another host machine so that the process of execution does not halt. There are two types of migration: live migration and non-live migration. In non-live migration, the VM from one machine is shutdown, copied to physical machine, and then rebooted at the host machine. This kind of migration has downtime. On the other hand, live migration is a process carried out without the downtime. Live migration is carried out in phases, namely, push phase, stop and copy phase, and pull phase. Push phase: the memory pages are copied which are unmodified/fresh from host to destination machine, while the VM is still running. Stop and copy phase: as the name indicates, the hypervisor stops the execution of VM and copies the remaining pages to the destination machine, and then the VM is instantiated. Pull phase: the new VM is instantiated in destination machine; when a page is being reached out and it is not present, then a page fault occurs, and it is been copied from host machine. VM migration is the core process to maintain the health of the data center. During migration, disk state, network state, and memory states are copied from host to destination machine. VM placement is a process of placement of VM for effective utilization of the data center. VM placements take into account intra- and inter-data center traffic, energy consumption of the machine, locality, and SLA compliance factor in order to provide high availability, load balancing, high reliability, and security.

18.3 Security Repercussions of the Compromise on Cloud Infrastructure

The security attack on cloud could give rise to security breaches such as data integrity violation, denial of service, manipulation of data, data ransom, data duplication, service-level agreement (SLA) violation, availability of data, confidentiality of data, trust issues, legal issues, accountability of resources, transparency, theft of service, and many more new concerns that are alarmingly increasing periodically.

Data integrity: A malevolent user who holds the access to data repository and manipulates the data in any form. In this case, data is said to lose its integrity. Data integrity refers to the consistency and accuracy of data in its original form. The attack on virtualized environment on cloud could lead to data integrity issues.

Manipulation of data: Certain protocols which are used for programming interface such as REST, SOAP, and HTTP are vulnerable to communication threats, and the user can make use of these loopholes to gain access to the environment and utilize this environment to manipulate the data.

Availability of data: Data is the necessary unit for any transaction or process to sail smoothly in any corporation. Data must be available all the time for handling of the processes. If an attacker has the possession of data repository, they can hamper the availability of data.

Denial of service: Cloud services are hampered by the possession of resources by the attacker, and when the requests for a resource come in from the user who needs it, the service request could be denied because of the illegal possession of the resources by the attacker.

Theft of service: The malignant user may get hold of the resources through a weak communication channel or port and steal the resources such as network, VM, computing power, etc. This affects the transparency of the services and creates trust issues between user and the cloud service provider (CSP).

SLA violation: Service-level agreement is a document which states the terms and conditions to avail the service and also states countermeasures which are to be taken when they are violated. SLA violation refers to the breaching of the contract and not abiding by it. This happens when the malignant user creates a user-specific attack and frames the CSP for the shortage of resources.

Resource accountability: As virtualization creates multi-tenant environment, isolation is a primary requirement to meet the accountability of the resources. The attacks such as DoS (denial of service) and DDoS (distributed denial of service) could assess the resource metering significantly wrong at both CSP and user side.

18.4 Literature

The literature provides us with the different works on virtualization and migration in VM [1, 7]. It discusses the kinds of attack that enables the malicious user to gain access to hypervisor. The author also sheds light on the threats pertaining to the virtual environment. The authors in [1] have done a thorough survey on the security issues and the available IDS for mitigating the attacks and the threats. The authors have given the bird's eye taxonomy of the security issues for the different service models [1]. They also discuss the proposed solution in literature in detail. Some of the existing proposals are Mirage, EVDIC, ImageElves, and OPS-offline. Mirage is an image management system where the authors have proposed secure mechanism to share the images with the help of access control framework along with filters to drain out unwanted information [11]. The advantage of Mirage is that it provides secure retrieval and storing of VM images and greatly helps in auditing. The drawback of Mirage is that the image handled is dormant type meaning, while execution, the state of the image might be compromised, but the attack would not be noticed till the image gets updated in the repository. Also, the framework does not comply with privacy and integrity. In [6], authors have discussed about another image monitoring system named EVDIC which uses encryption to secure the VM image. It uses AES encryption with $k = 256$ bit. EVDIC also stores integrity info of the VM image which is an advantage. However, EVDIC does not have the support for outdated software removal and owner's leftover data removal which are crucial to secure VM image. Authors in [13] have proposed a framework to provide VM security called VNSS. It contains components such as controller and multiple agents to secure the VM. Although the framework is implemented on Xen hypervisor, the scalability of the framework is still questionable. In [12], the authors have proposed a completely radical approach of trusting only the processor chip and the remaining components as untrusted. This framework gives good support for scalability, data privacy, and integration of the system. It takes help of both software and hardware to protect the system. Authors in [5] have used the VM introspection technique to propose Exterior. It is a dual VM architecture that pushes secure virtual machine (SVM) to host the guest VM (GVM). SVM executes kernel which is the same as GVM and redirects the memory state at hypervisor from SVM to GVM. This change gives the impression that the program is being run on GVM. This approach provides concrete security but is compromising on integrity of the hypervisor. The authors in [2] have proposed a technique for migration which is based on trusted computing. If the trust credentials are not favorable during launch process of VM, then the migration will not occur. The advantage of this approach is remote auditing facility. Authors in [10] propose a new architecture to overcome the drawbacks of old virtualization technology. This architecture introduces new blocks on the existing virtualization stack. This introduction provides security to some level but fails if the initiating hypervisor itself is affected putting all the VMs prone to attack. Taking the inspiration from the same architecture [10], authors in [3] have proposed a framework which introduces cryptographic encryption between VMM and the hardware and also make use of honeypots between VM and VMM. They bring in the extra layer of security between the hardware and hypervisor but also introduce delay for the key exchange while accessing the resource. All the above work in literature where in the solutions have been proposed keeping in mind only one parameter (e.g., hypervisor security or migration or VM image security, guest instance security). Nonetheless, the works did provide realistic solution toward security. We try to break the one-factor approach and intend to provide a framework which would provide solution to both virtualization and migration in VM.

18.5 Proposed Solution for Virtualization and Migration

We propose an alternate solution for the existing solution in literature for virtualization environment [10]. We have introduced the new modules upon the existing architecture such as Virtual Machine Integrity Monitor (VIM), Virtual Machine Resource Manager (VRM), and Dynamic Analyzer and Smart Decider for Virtual Machine (DASDVM).

18.5.1 Architecture

The proposed architecture is built on several assumptions and privileges. We assume that the host OS's kernel space can be held through special privilege access and can be accessed without interruption in the proposed architecture. We have introduced security monitors to overlook the protocols and processes in the VM and also VMM. Figure 18.2 illustrates the framework. The hypervisor communicates with the host OS which in turn communicates with the hardware through the kernel. The user could experience a delay, every time the hypervisor is listening to the hardware to nurse the needs. Hence we created a pool of resources that holds hardware-specific instantiation modules. This module helps to nurse hypervisor in case of hardware requirement. This module is placed in the kernel space of the host OS to efficiently carry out the process. Every time the VM needs a hardware resource, instead of giving interrupt signals to the hardware, the hypervisor could make use of the hardware device repository (HDR) to nourish the needs. The HDR is implemented as lightweight add-on module which can fire up the process of resource instantiation. We have proposed additional modules for providing additional security and smart management of the VM and VMM, namely, DASDVM, VIR, and VRM. The VRM handles the resource management of the VM and feeds the information to DASDVM, so that it can take intelligent decisions. The decisions will be based on the parameters such as current execution state, number of resources (clock cycles, cache, page hits, etc.), network congestion, and many more. The VRM listens to the status of the VM and records all the information. On the other hand, VIM is a security supervisor who checks the status of VMs, and if there are any possible attacks on any VM running on the same hardware, then it flags the VM and sends the information to DASDVM to not use the VM for further use and suspend the VM.

18.5.2 Components/Modules

DASDVM: The Dynamic Analyzer and Smart Decider for Virtual Machine is a module housed in the hypervisor to analyze the traffic, CPU cycles, workload, health of VM, and resource utilization of the data center. This is a logical analyzer and decision-making module that run when the hypervisor executes. This is a two-tier behavior analyzer and decision-maker. The functionality of the DASDVM is varied based on the parameters and the state of the machine. HIM: The Hypervisor Integrity Manager is a security monitor for the hypervisor that evaluates the security attributes. It maintains the log of hypervisors in the network to efficiently instantiate or shutdown the hypervisor based on the health of the VMM. VIM: The Virtual Machine Integrity Monitor is placed on the each virtual instance/guest OS. This is a lightweight module placed to monitor the cleanliness of the VM. VRM: The Virtual Machine Resource Manager is placed on each guest OS. It monitors the resource usage and the management of the VM.

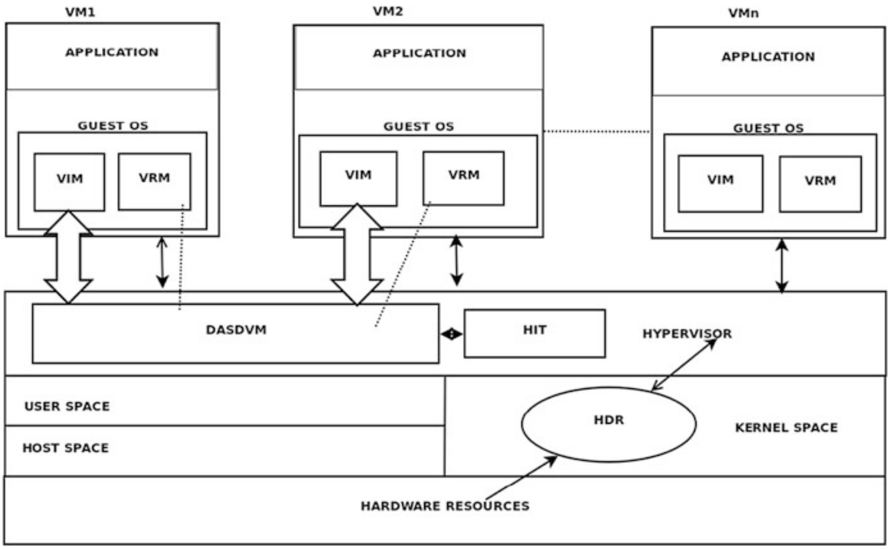

Fig. 18.2 Secure virtualized framework

18.5.3 Implications of Proposed Architecture on the Threats

The proposed architecture provides solution for the issues such as cross-VM side-channel attack, denial-of-service attack, and migration issues. The Cross-VM Side-Channel Attack: Cross-channel attack could be the implication of co-residency of VMs on the same hardware unit. The cross-VM side-channel attack could expose the information of cryptographic keys and network info to the attack user residing on the same hardware. Our approach consists of VIT module which indicates the worthiness of VM (VIT has integrity value which is stored as hash value and stored in the table), and it is fed to the DASDVM at periodic interval. This interval depends on the load of the DASDVM. Usually the time interval to feed the information is 7 s. If the value is low beyond the threshold (below 3, and the flag for high utilization from VRM is set), then sharing of information and resources between the VMs is prohibited by DASDVM, as this could indicate a possible compromise of the VM. Thus the VM is blocked from participation in the network. Denial of Service: DoS attack implies the resource wastage. The resources are being held by attackers who just pull out the resource anonymously. The resource, on one hand, is being wasted and, on the other, cannot be used when there is an actual need. Our approach takes care of this situation with the involvement of VRM module where it constantly monitors the usage of VM (network, bandwidth, data space). If the consumption is more compared to the previous needs (info log is maintained at DASDVM), then the DASDVM raises a ticket, and the user for which the VM is allocated should reply with the reason for the exceeding usage. The usage limit is set keeping in mind the previous instances (if the user is first timer, then the quota limit is set by

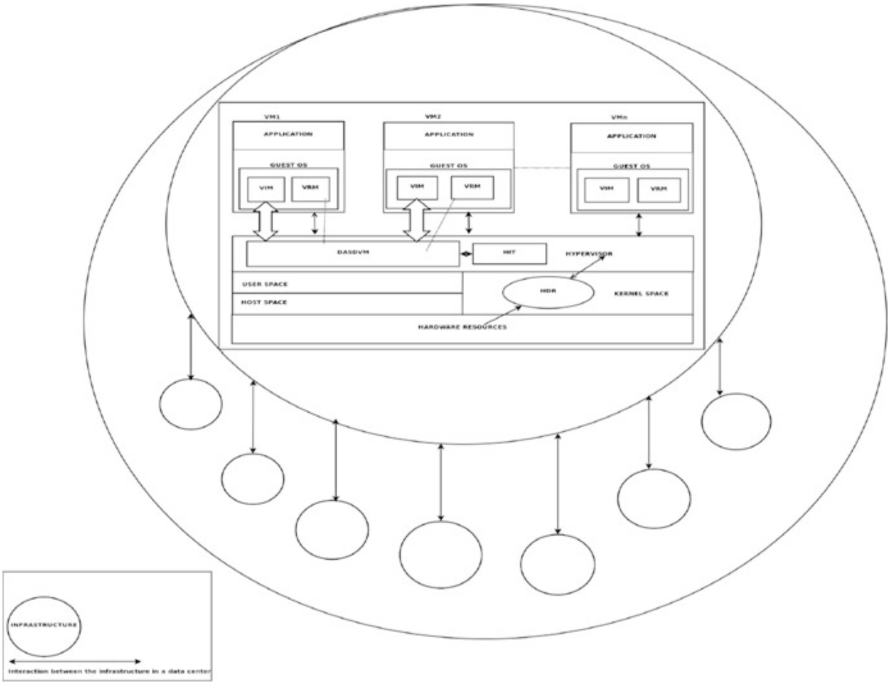

Fig. 18.3 Secure migration framework

the user). Likewise we can also solve resource accountability problem. Migration Issues: Migration of VM involves intricate parameters. Migration is carried based on network usage, legal issues, and architectural issues. Our approach, with the help of modules such as DASDVM and VRM, mitigates the migration challenges so as to effectively manage the data center. If the malicious attacker gains the access to VM and chooses to instantiate the VMM, then the running VM will be malignant. In order to avoid this situation during migration of VM from one network to another, HIM and VIM will be of significant use. The HIM indicates the purity of the hypervisor based on the values in the table (stored as hash value and contains the network ID, hypervisor ID, and the value). Likewise VIM indicates the purity of VM. The DASDVM will take the decision about the instantiation or management of hypervisor based on this information. While migrating, if the HIM/VIM value does not comply with the threshold value, then the migration will not occur, and the ID value of that particular hypervisor in the particular network will be blacklisted. This decision is taken care by DASDVM. This is illustrated in Fig. 18.3. The VRM gets the resource usage of the individual VM, and this info is fed to DASDVM. The smart decision-maker analyzes all these info and communicates with other network hypervisors (particularly DASDVM) and makes decision which will place the VM so that less overhead is incurred and effective resource utilization is also achieved.

18.6 Conclusion

In this paper, we have presented the security threats pertaining to virtualization and migration and the associated repercussions with the security issues of the respective layers. We have discussed the solutions in literature for virtualization and migration. We have proposed our own framework to handle the virtualization and migration. The introduction of add-on modules such as VIM, VRM, HIM, HDR, and DASDVM have improved the virtualized environment as well as support good live migration process. There is a scope of improvisation for this framework and is a work for future enhancement.

References

1. Ali, M., Khan, S.U., Vasilakos, A.V.: Security in cloud computing: opportunities and challenges. Inf. Sci. **305**, 357–383 (2015). https://doi.org/10.1016/j.ins.2015.01.025
2. Aslam, M., Gehrmann, C., Bjorkman, M.: Security and trust preserving VM migrations in public clouds. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE (2012). https://doi.org/10.1109/trustcom.2012.256
3. Bahulikar, S.: Security measures for the big data, virtualization and the cloud infrastructure. In: 2016 1st India International Conference on Information Processing (IICIP). IEEE (2016). https://doi.org/10.1109/iicip.2016.7975336
4. Bauman, E., Ayoade, G., Lin, Z.: A survey on hypervisor-based monitoring. ACM Comput. Surv. **48**(1), 1–33 (2015). https://doi.org/10.1145/2775111
5. Fu, Y., Lin, Z.: EXTERIOR. ACM SIGPLAN Notices **48**(7), 97 (2013). https://doi.org/10.1145/2517326.2451534
6. Kazim, M., Masood, R., Shibli, M.A.: Securing the virtual machine images in cloud computing. In: Proceedings of the 6th International Conference on Security of Information and Networks - SIN '13. ACM Press (2013). https://doi.org/10.1145/2523514.2523576
7. Khan, M.A.: A survey of security issues for cloud computing. J. Netw. Comput. Appl. **71**, 11–29 (2016). https://doi.org/10.1016/j.jnca.2016.05.010
8. Latif, R., Abbas, H., Assar, S., Ali, Q.: Cloud Computing Risk Assessment: A Systematic Literature Review, pp. 285–295. Springer, Berlin (2014). https://doi.org/10.1007/978-3-642-40861-8_42
9. Rawat, S., Tyagi, R., Kumar, P.: An investigative study on challenges of live migration. In: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE (2016). https://doi.org/10.1109/icrito.2016.7784939
10. Sabahi, F.: Secure virtualization for cloud environment using hypervisor-based technology. Int. J. Mach. Learn. Comput. **2**, 39–45 (2012). https://doi.org/10.7763/ijmlc.2012.v2.87
11. Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P.: Managing security of virtual machine images in a cloud environment. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security - CCSW '09. ACM Press (2009). https://doi.org/10.1145/1655008.1655021
12. Xia, Y., Liu, Y., Chen, H.: Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks. In: 2013 IEEE 19th International Symposium on High Performance Computer Architecture (HPCA). IEEE (2013). https://doi.org/10.1109/hpca.2013.6522323
13. Xiaopeng, G., Sumei, W., Xianqin, C.: Vnss: A network security sandbox for virtual computing environment. In: 2010 IEEE Youth Conference on Information, Computing and Telecommunications, pp. 395–398 (2010)