Possible Solutions for the Drawbacks of Data Center Security Mechanisms

V.S.P Vidanapathirana, M.S.T.J Nanayakkara, A.M.S.D Attanayake, V.Abenayan, Pubudu Dhanushka, Dhishan Dhammearatchi

Department, Institute Name, if any Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Abstract- As the place that stores the brain in an organization, a Data Center centralizes the operations of the company, its equipment and stores, maintains, propagate the data that runs through the company. Data Centers may have a physical or virtual infrastructure and data which are stored in them provides the base for the successiveness of an organization since they are much valuable when making decisions in the business processes. In simple terms, the past, present and the future of an organization relies on the outcome of the analyzed data. Due to these reasons, it is one of the top priorities of a company to ensure the security and reliability of data centers and their information. With the advancement of the technology, securing the data centers to its best level has become a complicated task, due to the various possible attacks. Making an attack on a data center becomes easier when there are loopholes in the security mechanisms that are used in data centers. In this paper the authors describe about the existing security mechanisms which are specific to the physical data centers. Furthermore, this paper has discussed the possible solutions that can be used to ensure the security of data centers as a perspective to the current Information Technology (IT) industry.

Index Terms- Data Center, Data, Data Center Security, Security Mechanism, Physical Data Center

I. INTRODUCTION

The complexity of the world increases by the minute of the day, due to the effects of globalization which is a combination of the improvements made on information technology and telecommunication. The potential of globalization has generated a huge advancement in the industry of information technology and it has made the world a universal ground which keep people connected from all corners of the world. In simple terms, this rapid growth in the field of Information technology is a worldwide phenomenon experienced today.

The emergence of computer networking methodologies plays a key role in the global IT boost, unfolding a new era of communication technology. The global private sector was the first to explore the endless opportunities and networking by residing the business processes with the integration with data centers to have the competitive advantages in the business world. Today, the ability to achieve the organizational goals relies purely on the availability, efficiency and authenticity of the information. It is a well-known fact that such information should be protected by all means because in the present business world, it can be defined as one of the most valuable assets in an organization since some of the future decisions that are to be made totally rely on them. Therefore, the security of the data centers falls to the topics that get the major attention and the concern in an organization.

As a highly dynamic and technical field, data center security deals with all the aspects of securing the data centers from intrusions. Hacking, Distributed Denial of Service (DDoS) attacks, physical attacks are some of the common issues that threatens the security of data centers and sometimes, well-designed, fully protective security mechanisms may not have what it takes to prevent such attacks. Confronted with this particular scenario, the authors has chosen to indicate a great diversity of data center security, more specifically the draw backs in the data center security mechanisms in the current IT industry.

Same as in every other concepts in life, globalization has its pros and cons. It bring the whole world together under one roof but at the same time it makes them vulnerable by exposing the sensitive data to unauthenticated, unauthorized parties who are eager to abduct, change or use those data in an unwanted manner. Ultimately, such acts can increase corruption, extortion, racketeering and violence and can be abused to launder money, to commit fraud and to enable illicit activity and irregular movement for organized crime purposes [1]. This is much dangerous than it is in the real world since the cyberspace is a borderless realm that anybody with an internet facility can put hands on.

Therefore, throughout this paper it is the intention of the team to discuss and present a perspective on the possible solutions that can be used to avoid these threats and vulnerabilities that data centers are facing in the current industry of IT while briefly going through the existing data center security mechanisms.

The rest of this paper is organized as follows. Section II has provided the existing related work. Section III describes the objectives of conducting this research and the Discussion of is given in Section IV. The Conclusion is presented in Section V.

Literature Review

Kumar S. and Padmapriya S (2014) has presented a survey based conclusion regarding the varieties of clouds, common drawbacks of cloud storages, more specifically about the security threats that cloud storages face and its vulnerabilities [2]. It has described about the top nine security threats as identified by the Cloud Security Alliance (CSA) in 2013. According to that, Data Breaches, Data Loss, Account Hijacking, Insecure application programming interfaces (APIs), Denial of Service, Malicious insiders, Abuse and Nefarious Use, Insufficient Due Diligence, and Shared Technology Issues are the nine major security issues

that can threaten the cloud storages. Apart from that, it has mentioned several solutions to each and every security threat mentioned previously.

Juels A. and Oprea A. (2013) has provided a set of techniques that can be used to secure the cloud data [3]. It has proposed an auditing framework that gives the tenant visibility in to the correct operation of the cloud, which can help the cloud to enhance the security. At the end they have discussed about the remaining issues of cloud computing as directions to new research areas, such as performing computations over tenants 'encrypted data, ensuring tenant isolation and geo-location of data.

Barroso L. Clidaras J. et al (2013) has lengthily discussed about the data centers and how it can be used as a computer [4]. It has stated that the large data centers that can be seen in the industry nowadays differs from traditional hosting facilities in the past. Such data centers are complex than the traditional data centers of earlier times and therefore they cannot be considered as a set of co-located servers and the security mechanisms that work on this kind of large data centers are critical and should be stronger as well.

Barron C. and Yu H. et al (2013) has mentioned about some of the cases happened regarding real world companies, who became victims of cloud storage attacks [5]. Under that they have vividly discussed about social engineering attack, Extensible Markup Language (XML) signature wrapping attack, malware injection, data manipulation, account hijacking, Synchronization (SYN) flood, and wireless local area network attacks. The solutions or the steps that the companies have been taken has also been stated in here, such as presenting an algorithm to detect malicious packets, and another algorithm to prevent such malicious packets spreading through the cloud network.

Kumar V. and Swetha M. et al (2012) has presented a survey based idea about the data security mechanisms in cloud computing [6]. It has described about the possible security issues that can combatively threat the cloud data, which may delay its adoption. It has high-lightened the security mechanisms that are enforced or invoked by the major cloud service providers such as International Business Machines (IBM), Institute of Electrical and Electronics Engineers (IEEE), Amazon etc. It has concluded that it is a need in a cloud service to analyze the data security risk before putting the sensitive or critical data in to a cloud storage environment.

Meixner F. and Buettner R. (2012) has provided an overview regarding the trust in cloud computing [7]. When surfing the online world, security and trust are mapped together and it states that those two components are integral parts in cloud computing which are needed for its adoption as well as the growth. It also has shown that using the existing technologies in the best manner can build the trust measuring tools and in the bottom line of this state, using such tools with the means of technologies can improve the security in cloud computing.

Ayoleke I. (2011) has mentioned that even though the concept and the practical aspect of cloud data storages seems enthusiastic, there are much facts to be cautious about [8]. It has vividly described about the security issues that Cloud Deployments Models, Private cloud, Public cloud, and Hybrid cloud could face, and the possible challenges against cloud computing regarding security, costing model, charging model etc. in a detailed manner. At the end, it also has stated that cloud computing has the potential to become a prime-runner in the IT industry, as a secure, virtual and financially feasible IT solution.

Shaikh F. and Haider S. (2011) has mentioned that the only drawback of the cloud data storages is the lack of security [9]. The safety and security of the cloud data storages can be assured by the mutual interest and effort of the clients and the service providers. It has identified that the top security concerns of cloud data storages are Data loss, Leakage of Data, Client's trust, User's Authentication, and Malicious users handling. The researchers has proposed a new governance, risk management, and compliance stack for cloud computing called Cloud Security Alliance (CSA). These security tools can be downloaded by the organizations for free of charge and lead them to develop public and private clouds according to the industry standards in a secured approach.

Wang C. and Wang Q. et al (2010) has discussed about ensuring the data storage security in Cloud Computing, which is fundamentally a distributed storage system [10]. It has proposed an efficient and flexible distributed scheme that includes an accurate dynamic data support extending to block append, update, and delete in a secure manner. It relies on the eradication revising code in the file distribution preparation to give repetition equality vectors and grant the data perseverance. By using the homomorphic token with distribution verification of erasure coded data, the described scheme accomplishes and ensures the reconciliation of the accuracy in the storage, and data error localization. With the use of a descriptive and effective security and performance analysis they have showed that the schema presented is highly capable and strong towards the Byzantine failure, malicious data modification attack, as well as server intriguing attacks.

Zhang Q. and Cheng L. et al (2010) has surveyed about the state-of-art in Cloud Computing its most important concepts, characteristics, architectural designs, key technologies, security mechanisms as well as the research areas [10\1]. Those facts are presented in a lengthy descriptive manner, providing the opportunity of better understanding about Cloud computing.

Gong C. and Liu J. et al (2010) has discussed about the characteristics of cloud computing including the methodologies that can be used to design, develop and adopt a cloud computing system [12]. The loose coupling and strong fault tolerant have given as the major technical characteristics. Briefly it describes about the security of cloud storages as well as how it can be used for an organization in their business processes.

Okuhara M. and Shiozaki T. et al (2010) has explained how the customers can get the full benefit of cloud computing without worrying, by implementing the proper security measures [13]. It also has mentioned about the security issues that threatens the well-being of the cloud storages and defined about the Fujitsu's security architectures that can be used to solve those issues. Fujitsu security architecture has the ability to support for drafting security policies and as a part of consulting menu for businesses which are moving on to cloud computing it has given the capability to develop the security strategies as well.

Yuefa D. and Bo W. et al (2009) has presented a security model for cloud computing while analyzing and describing the data security issues that matters to cloud data storages, and the importance of enhancing the security in data storages as well

[14]. By utilizing the Hadoop Distributed File System (HDFS) the researchers have gotten the requirements of the security of the data stored in cloud data storages and they have suggested a mathematically provable data model for cloud computing.

Greenberg A. and Hamilton J. et al (2008) has provided an approach to significantly improve data center efficiency in a cost effective manner [15]. The cost of a data center are concerned with the servers, infrastructure, power requirements, security methodologies and networking, and since the costs are steep, the use of a data center can be low. Due to this reason, the researchers have been provided a simple set of steps that can be taken, as a solution for this issue. Increasing the quickness of the internal data center network, in order to fight the resource fragmentation has given as the first step in that procedure. As a method of reducing costs it also plans to get more work from less number of servers. Secondly, the design of algorithms and market mechanisms should be considered to increase the efficiency of data centers. In order to improve the reliability in the event of failures, Geo-diversifying data centers can improve end to end performance which can be described as the third and the final step. To retrieve the financial profits from the Geo-diversity new systems should be built to manage its state, as well as the joint optimization of data center and network resources.

Yaar A. and Perrig A et al (2003) has described about a path identification mechanism called “Pi”, which can be specifically used as a security mechanism against the DDoS attacks [16]. This mechanism has the components of IP Traceback methods which is concerned with marking the victim to attacker paths with unique markings rather than reconstructing that path. In that manner, the victim will be given the capability to identify and filter on a per-packet basis, any incoming packets that is similar to the pre-defined attacker marks.

II. OBJECTIVES

The following can be considered as the objectives that the authors are trying to achieve via this research.

- Identify the definition and the usage or the importance of data centers.
- Recognize the security mechanisms that are currently in use to ensure the security of the data centers.
- Analyze the drawbacks in the existing security mechanisms.
- Discuss the possible solutions that can used to overcome the issues identified.

III. DISCUSSION

Data Centers are typically large facilities that takes a huge space in a dedicated building (server farm) or else in a space that company paid for. Unlike cloud, it is in a physical surface, which makes it vulnerable to both internal and external attacks. Therefore it can be clearly stated that the security of them can be at a risk, along with the data that company stored in them. Understanding the possible solutions to assure the security of the data centers can be an aid to minimize that risk. In the following content the authors have vividly described such techniques that can be used to ensure the security of the data centers.

Stage-wise provisioning

Network provisioning systems can be defined as intermediary tools that is useful when performing tasks like customer services, log transactions, carry out requests, and update files [17]. Implementing such provisioning system in a data center can give the permission to the customers to install the hardware before the connectivity of the network become to the state ‘available’, which means that the providers have enough time execute any initiations as the desire before they are given the capability to interact with different hardware from all corners of the world. A person who might try to dispatch this kind of assault would most likely do as such with the ambition of executing remotely. This brings the conclusion that the contracts that are being made for customers to facilitate the data centers should be defined in a manner which allows them to use it in a one or two weeks of provisioning period. During the given period, initiation of the hardware materials, and background checks can be carried out without any issue.

Facilitating in the tier-level

It is a known fact that the new clients who are at the very beginning of their business do not have range of requests as the large business owners do. The requirement of the volume of rack space varies from one to another but according to that, facilitating can be done in a separate manner. Due to that manner, the low-tier clients will be able to host the data center in a place that includes a less-critical framework. This gives the low-tier clients to host the data center in a low-profiled manner, or in other words outside the critical areas where there is a high possibility of commencing attacks.

Proper Maintenance Process

Proper maintenance is one of the significance methods that can be used to improve the security of the data centers. This evolves with several steps.

One is, providing the authentication levels to all the documents, telephone calls and other identification mechanisms related to the data center maintenance. It is necessary for the company to record all the telephone calls as a log, which allows them the opportunity to trace back in an event of suspicion. When interacting with the vendors, it is essential to ensure it is possible to reach the particular vendor using the number which is already on the file. It is true that reaching out via cellular is easier, but when it comes to security it is always better to accept maintenance requests unless it is a land line that can be traced back. When authenticating the documents, such documents should be checked with the formal documentations which will give them the opportunity to compare or check whether that it is already on the file.

The maintenance of the data centers should be done in a centralized manner. The maintenance appointments should be checked properly and should go through the data center manager to further clarification. The vendors who are in the supplement of maintenance services should be checked with the telephone, to

ensure whether they are already registered under the maintenance appointments. These teams should be provided with a unique identification mechanism such as a password or face recognition method to verify themselves before entering the data center.

Each and every entering to the data center should be scanned deeply, to ensure that there is no any entering of an explosive. This can be done by a well-trained K-9 or using a portable detection device that is capable of detecting the explosives. The people who are responsible to detect such should have a sharp eye that does not miss any entering that happens with a suspicious looking device or tool. The bomb radiation detecting devices can come in handy in a situation like this, which have the ability to scan all the incoming tools or devices. If the equipment come in a box they it should be unpacked and scanned in an internal manner and it is essential to note that the regular chasses usually has only a simple latch which can be easily opened.

The data center maintenance should be done in a supervised manner. A small group of people can be allocated for this purpose. It does not matter that the members in that group is rich with technical knowledge related to data centers but they should have the basics like the components of the data centers and the tools and equipment that is being utilized when there is a maintenance. The instinct of identifying unusual acts happen during the maintenance is the key qualification in this kind of role.

Relationships that comes in an informal manner should not be trusted, and also should not be encouraged. Avoiding such situations is always better when it comes to ensuring the security of the data centers. Being familiarized with the vendors is fine, but allowing vendors to bring guests is not a good idea unless the vendor has cleared them. As mentioned previously, the unique credentials given to each and every vendor should be check at each appearance they make.

Continuous Monitoring Process

Keeping the data centers monitored is another way to ensure that they work in their best manner, and also detect if there is an anomaly that works irregularly. When something goes off the rid of the regular pattern, it should be checked deeply. For an example, if a customer is pulling a little amount of data and if it shows a high traffic, it is something to be suspicious about. On the other hand if it displays an unusual traffic pattern in an irregular hour it is also something needs to be checked out. The common sense and the instinct is important in this task as well. Investigating the traffic in Internet Protocol (IP) level has the ability to recognize the number of unique hosts that are interacting with the tools and equipment of the customer. If there is a less number of hosts in comparison to the number of equipment, it is nothing to worry about.

Being Aware of the Customers

The company or the responsible parties should be aware of the customers who are attempting to enter to the data center facilities. The authority of entering or accessing the data centers should only be given to the regular customers, not just because their name is already in the file, but because the company received positive results regarding the profile of the customer during the background check that was carried out. The relationship between the company front and the customer must always be conducted in an official manner, because it will avoid the attempts of the customers who are attackers behind the mask to build long term relationships in order to reach their targets.

The new customers should be interviewed properly, and their history must be reviewed as well. It is necessary to find out whether the customer company's need for this data center, not just in a general manner but in a specific manner. The company should go in to the root of that particular customer to realize whether the customer does not seem to be aware of the business, and ongoing projects it automatically sends an alert to the company that this customer should be examined thoroughly. The company should get an idea about the customer website, whether it exists or not, how they are willing to do the payments for the necessary services, whether the customer is a registered company, or whether they have a valid business license, and how long has it been from the first opening day of the company. If these questions are answered positively or if it is a known company for several years, with multiple branches or staffs instead of being a company that runs virtually or in the residence address, the risk can be considered somewhat lower. Even after giving the authority to access the data center, it is important to check them often and it is company's authority to dismiss the permission that is being given to the customer if they are making attempts to broadcast pornography, send spams etc. Justifying the customer as a responsible business is one way to accept the new customers.

Assessing the Company Externally

There is a pretty good chance that some of the issues that lies within the relationship between the data center facilities and the customers cannot be seen internally. As a solution for this scenario, the company can hire an external party, which they analyze the interaction that the customers and data center has, as well as how effectively does the management of the data centers takes place in the company. Apart from that, to inspect the strength or to evaluate the robustness of the defense mechanisms that is being used on the data centers, the company can hire another trusted party to send them a mock attack to check how adequately does the data center defense themselves, and the level of survival. This kind of assessments done by external parties with some misdirection will help the company to enhance the security of the data centers, as well as to recognize the weak areas of them which gives them the opportunity to apply new security techniques that were not there before.

Hardware Inspection Policies

The most fundamental policies should be added to the data centers, especially the ones specified for the hardware and equipment. Such policies must be introduced and stored in the data centers to prevent customers from suggesting harmful explosives and other devices. This should be added as a sector to the contract that company presents to the customer and it is important to note that the company owns the authority of checking the external devices or the hardware equipment that customer is attempting to introduce to the data center facility.

This situation also extends towards the behavior of the customer when they are utilizing the data center facility. The customer should treat the facility with care and responsibility,

and they are obliged to take the blame for any physical damage they cause. The customers cannot leave the data center with loose power cables, broken devices or with any other cause that brings physical damage to it. The policy should justify all of these matters.

As mentioned previously, there are many tools that can be used to detect the explosives and also a team can be given the k-9 training to detect 11 types of explosives separately. The close and continuous monitoring is the key to assure that the customer do their duty up to the hardware policy mentioned in the contract.

Preventing the Unauthorized Building Access

The office building should be protected by its all cost, therefore only the authorized parties should be allowed to walk in. It is always better to accompany them with some trusted officers of the company while the customers carry out their work because that may make the attacker behind the mask of a customer hesitate from doing something harmful.

In most companies, the rooftop is where all those antennas and satellite machineries are located. These areas should not be allowed to customers to simply walk in and make use of. If access given under some circumstance, it should be during the regular working hours and under the close supervision of a member in the company. Using this kind of technique will avoid the data center from being an easy target.

IV. CONCLUSION

Data Centers are one of the finest pieces of technology that takes the responsibility of storing the data in a company in an efficient manner. It is one place that a company can rely on when it comes to making decisions to the future, and that is what makes it critical as well. Due to the speediness of the technology around the world, these data centers has become another place that an authorized personal can attack, steal and utilize those data in an unnecessary manner. It is true that there are many security mechanisms that guard the data centers but, there are plenty of drawbacks in them as well. Therefore, it is important to be aware of the attacks that threatens the security of the data centers and the techniques or the possible solutions that can be taken to avoid such threats. Throughout this paper, the authors have explained about the existing security mechanisms in a descriptive manner and stated down the possible solutions that can be done to avoid their drawbacks as well.

REFERENCES

[1] "Emerging Crimes", Unodc.org, 2016. [Online]. Available: https://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html. [Accessed: 13- Feb- 2016].

[2] S. Kumar, and S.Padmapriya, “A Survey on Cloud Computing Security Threats and Vulnerabilities", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 2014. [Online].Available: http: //www.ijireeice.com/upload/2014/january/IJIREEICE3C___a_padma_A_survey.pdf. [Accessed: 09- Feb- 2016].

[3] A. Juels and A. Oprea, "New approaches to security and availability for cloud data", Communications of the ACM, vol. 56, no. 2, p. 64, 2013. [Online]. Available: https://www.emc.com/collateral/white-papers/h12759-wp-security-availability-cloud-data.pdf. [Accessed: 10- Feb- 2016].

[4] C. Barron, H. Yu and J. Zhan, Cloud Computing Security Case Studies and Research, 1st ed. London, 2013. [Online]. Available: http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf. [Accessed: 12- Feb- 2016].

[5] L. Barroso and U. Hölzle, The datacenter as a computer. [San Rafael, Calif.]: Morgan & Claypool Publishers, 2009. [Online].Available: http://www.morganclaypool.com/doi/pdf/10.2200/S00193ED1V01Y200905CAC006. [Accessed: 08- Feb- 2016].

[6] V. Kumar, S. M.S, M. M. S. and P. S, Cloud Computing: Towards case study of Data Security mechanism, 1st ed. 2012. [Online]. Available: http://www.ijater.com/Files/IJATER_05_01.pdf. [Accessed: 08- Feb- 2016].

[7] F. Meixner and R. Buettner, Trust as an Integral Part for Success of Cloud Computing, 1st ed. 2012.

[8] I. Ayoleke, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[9] F. Shaikh and S. Haider, "Security threats in cloud computing", Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pp. 214-219, 2011. [Online] Available: http://fs3.dajie.com/2012/08/13/031/13448264310678702.pdf. [Accessed: 12- Feb- 2016].

[10] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010 Proceedings IEEE INFOCOM, 2010. [Online]. Available: https://eprint.iacr.org/2009/579.pdf. [Accessed: 11- Feb- 2016].

[11] Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges",Journal of Internet Services and Applications, 2010. [Online]. Available: http://Cloud computing: state-of-the-art and research challenges. [Accessed: 09- Feb- 2016].

[12] C. Gong, J. Liu, Q. Zhang, H. Chen and Z. Gong, "The Characteristics of Cloud Computing", 2010 39th International Conference on Parallel Processing Workshops, 2010. [Online]. Available: http://www.mashad.post.ir/_ITCenter/Documents/TheCharacteristicsofCloudComputing_20140722_154207.pdf. [Accessed: 10- Feb- 2016].

[13] M. Okuhara, T. Shiozaki and T. Sazuki, Security Architectures for Cloud Computing, 1st ed. FUJITSU Sci.Tech, 2010. [Online] Available: http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol46-4/paper09.pdf. [Accessed: 13- Feb- 2016].

[14] Yuefa, W. Bo, G. Yaqiang, Z. Quan and T. Chaojing, Data Security Model for Cloud Computing, 1st ed. 2009. [Online]. Available: http://www.academypublisher.com/proc/iwisa09/papers/iwisa09p141.pdf. [Accessed: 13- Feb- 2016].

[15] A. Greenberg, J. Hamilton, D. Maltz and P. Patel, "The cost of a cloud", ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, p. 68, 2008.

[16] D. Abraham Yaar, "Pi: A Path Identification Mechanism to Defend against DDoS Attacks", In IEEE Symposium on Security and Privacy, 2003.

[17] "What is provisioning? - Definition from WhatIs.com", SearchSOA, 2016. [Online]. Available: http://searchsoa.techtarget.com/definition/provisioning. [Accessed: 01- Mar- 2016].

AUTHORS

First Author – V.S.P Vidanapathirana, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Second Author – M.S.T.J Nanayakkara, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Third Author – A.M.S.D Attanayake, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Fourth Author – V.Abenayan, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Fifth Author – Pubudu Dhanushka, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Sixth Author – Dhishan Dhammearatchi, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka