Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

Review

REVIEW STUDY OF E-MANAGEMENT BARRIERS, CHALLENGES AND SECURITY

Arwa Y. Al-Eryani.
Yemen Academy for Graduate Studies, Yemen

Article info

Article history: Accepted

August, 2014

Keywords:

E-management

Barriers

Security

Abstract

This study aims to review papers focusing on e-management barriers, challenges, and security. Most of the results present in the literature showed the importance of e-management but also found out that it faces many barriers and challenges such as Security, Trust, Privacy and Awareness. Many studies should be made in order to overcome the barriers facing e-management to gain its great benefits.

* Corresponding author: Dr.Arwa Y. Al-Eryani.
Tel. +967 1 404077; Fax: +967 1 467919
E-mail address:arwa_y@hotmail.com

Introduction

In this era, information is considered as a strategic critical resource for generating value-added products and services. The shift of societies towards the information society has had deep effects on numerous aspects of human life such as economic, social and cultural aspects [1].The impact of information technology on human societies is not less than that of industrial revolution, therefore the information technology developments and its application is regarded as the fourth digital revolution [2].

As information technology grows, e-business applications are found all over the world. More and more companies recognized the benefit of e-business and moved from traditional business to e-business [3]. E-management is the new way to manage all e-business applications [2].

The author has reviewed much e-management literature but it seems that there is not sufficient number of research works done in this field. E-management can play a role in e-business and e-commerce [4]. We use the term "e-management" to broadly describe the publishing of information and the performing of various transactions over the internet, extranets, or intranets. It seems that the Internet and e-business have changed the way firms conduct business globally using e-management [5]. In this review study, e-management will be discussed as the new management method in the organizations implementing e-business to its functions.

Study Methodology

The methodology which was used in this study was based on reviewing papers written about the barriers, challenges, success factors, and security impact on e-management implementation.

Conception of e-management

E-business or electronic Business, is the administration of conducting business via the internet. This would include the buying and selling of goods and services, along with providing technical or customer support through the internet [4]. E-business is also a term often used in conjunction with e-commerce, but includes services in addition to the sale of goods. Furthermore, E-business is the application of information and communication technologies (ICT) in support of all the activities of business [6]. Commerce constitutes the exchange of products and services between businesses, groups and individuals and can be seen as one of the essential activities of any business. In the other hand, e-management means the electronic management of all business issues [7]. E-management will be critical for ensuring that e-business applications are available for customers [8]. The implementation of e-management is related to all the employees of the company. That is why we have to consider the human factor as the most important factor impacting e-management [6]. E-

management has many benefits such as the elimination of distances through providing linkage among separate computers in the world-wide web, and the computerization of systems and telecommunication which result in new capacities to transfer sounds and images [7].

E-management ensures the best utilization of resources, increases efficiency, and provides support to high management in planning, and managing human and financial resources [9].

E-management can play a role in e-business & e-commerce management, and gain some benefits such as [4]:- reducing costs, improving product or service quality, reaching new customers or suppliers, creating new ways of selling or providing existing products and services.

Barriers of e-management

Seresht et al. has studied the barriers and challenges in Iran [7]. They indicated that the e-management is an umbrella name for several e-business modules. Their methodology was based on interviews and questionnaire. The research population was the public organization and the sample was 200 experts, scholars and managers in 45 public organizations. The research hypotheses were:

- Managerial factors hinder the utilization of e-management in Iran
- Humanistic factors hinder the utilization of e-management in Iran
- Socio-cultural factors hinder the utilization of e-management in Iran
- Organizational-structural factors hinder the utilization of e-management in Iran
- Technical-technological factors hinder the utilization of e-management in Iran.
- Environmental factors hinder the application of e-management in Iran.

They have addressed the following barriers which have impact on e-management implementation in Iran:-

Managerial Factors including:

Lack of technological awareness among managers, lack of computer-relevant knowledge and experiences of managers, lack of awareness among mangers about the advantages of IT, lack of motivation and support for managers, insufficient commitment of top managers in IT implementation and short life-cycle of management.

Humanistic Factors including:

Lack of IT specialists in organizations, employees` lack of interest and motivation to apply new techniques, lack of relevant training for employees and employees` resistance to change.

Cultural-Social Factors including:

The non-developed culture for proper application of IT, unfamiliarity of users with IT and unfamiliarity of citizens and authorities with IT performance.

Organizational-Structural Factors including

Weakness of communication channels in organizations, lack of financial resources to equip software and hardware and insufficient financial capability of units to apply IT.

Technical-Technological Factors including

Lack of sufficient software facilities, incongruity between systems and users, lack of sufficient band-width for internet, existence of network and telecommunication problems and difficulties in IT application.

Environmental Factors including

Absence of an integrated network in country, lack of necessary rules and regulations in the country, lack of clarity in policy-making in IT and lack of coordination and cooperation between different units and divisions in industries and organizations.

Challenges of e- management

Chaffey et al. [4] addressed some of e-management challenges which work on e-management such as:

- Expanded competition.
- Increasing Customer power.
- Network security.
- Reliability of website technologies and network uptime and speed.
- Back office integration.
- Expense of infrastructure and uncertainties over return on investment (ROI).
- Lack of in-house expertise (outsourcing is common, but managers may lack expertise to make good decisions).
- Rapid change makes it hard to know when to “leap in” and invest.
- Difficulty in establishing customer trust in a virtual world.
- Cross border transactions/sales territory agreements.

Li et al. [10] concluded that small and medium sized businesses use the internet and networked application to reach new customers and serve their existing ones more effectively. It depicted that the security is the biggest challenge facing small and medium sized businesses. According to Bichler [11] the top 5 security issues are worms and viruses, information theft, business availability, the unknown and security of legislation

Jingting et al. [3] studied the factors affecting e-business success with impact on e-management as well. How other companies can learn from the successful ones?

They made an exploratory study on the factors influencing e-business success. Firstly, 52 factors are suggested. Secondly, two rounds of survey with Delphi method are conducted. Qualitative and quantitative analysis were used to identify 57 factors.

These factors were into categories: - Leaders, management, organization, technology, customer and Supplier.

They discussed that leaders should participate in the project and establish a clear target, be-

cause only with their support can the project be successful [3]. Leadership also indicates establishing an e-business strategy.

Also they discussed the role of management in the organization. Management plays a key role in implementing e-business. Only an effective management can represent the advantage of e-business system. The third factor is the Organization and its capabilities. It is interrelated with leadership, management and technology. Implementing e-business will bring many changes to a company because the existing organizational structure and processes found in most companies are not compatible with the system [12].The current organizational structure must provide an environment that is well suited for e-business. Company should reengineer business processes to link to life events at the front end and link to existing legacy processes and system at the back end. The fourth factor is technology. E-business combines business and technology. Without good IT infrastructure, companies cannot fit the evolution of e-business.

Last factor was Customer and Supplier. They have to ensure that e-business is related to suppliers, customers and other companies that involved in the business process. Having a good relationship with the partners is important for success.

Al-Malik [9] studied the impact of e-management in Saudi Banks, he came with the result that e-management assists in providing all required information on banks, bank services, and high management support in information technology.

E-Management Security

One of the most important factors in technology is security and privacy. Many potential customers still cite concerns about security as the most important issue stopping them from engaging in more electronic business [13]. Security is not optional; companies must consider it as they move to deploy e-business [6]. The widespread adoption of e-business and e-management has brought with it serious new organizational security concerns [13].To e-business security plans are unique and must be developed through a series of steps [8]. E-management depends on providing customers, partners, and employees with access to information, in a way that is controlled and secure. Managing e-business security is a multifaceted challenge and requires the coordination of business policy and practice with appropriate technology [6].

Lichtenstein [14] has identified e-business security management practices which will reduce such policies and procedures more effectively. In particular, his study focused on the importance of the human issues in determining such policies and procedures, and the use of a universal e-business security policy to manage the risks and other issues.

In all companies studied (four Australian and one American), he discovered evidence of Internet risks of various types[14].These risks

were affecting the companies to different degrees, indicating the existence of a serious e-business security problem in Australian companies [14]. A major finding in Lichtenstein study was the importance of human issues (for employees) in e-business security. The two main human issues were: freedom of Internet use, with employers needing to limit Internet usage to manage the non-business usage risk; and privacy, with employees believing in the right to privacy of Internet use, hence opposing the monitoring of web accesses and email.

They found [14] other human issues to be of concern, in particular:

- Censorship: filtering of sites from employee access via firewalls and other mechanisms, was not popular with employees at the companies studied;
- The right to be kept informed: employees were suffering from a lack of awareness of security risks, needs and policy;
- Accountability: employees were not being held accountable enough for their Internet actions, due to a lack of policy, policy implementation technology, and monitoring resources.
- Trust: employees were concerned about the lack of trust shown in them by their employers through various policy decisions.

Security is the counter to the necessity of opening the enterprise to the great wide world of the Internet which is associated, anyway, with e-business and e-management [14].

Narendra et al. [8]: came up with the 10 Stages Security Management:

1. Identify security plan.
2. Evaluate risk.
3. Evaluate expenses.
4. Find attacker.
5. Decide security vulnerabilities.
6. Evaluate technologies.
7. Consider attacks detection.
8. Decide action on attacks.
9. Educate employees.
10. Appraise insurance.

Discussion

From these papers which have their main ideas and results summarized, the most important barriers of e-management can be listed as:

The managers play a vital role in the organization. In the same time, they are considered as one of the barriers of implementing e-management. Lack of technological awareness among them as well as lack of computer knowledge and experience, and little or no awareness of the advantages of IT make them less motivated to support e-management.

As have been mentioned before the human is the most important factor of success when applying e-management. On the other hand there are many barriers related to humanistic factors. Such as lack of IT specialist among them, lack of interest in IT and lack of relevant training. These factors create resistance to change in the organization.

Many countries, especially developing countries have many socio-cultural factors that are considered as barriers to the e-management's implementation; Such as the unfamiliarity of citizens with IT, while they have to be part of the new environment and share in dealing with e-business. Also the weakness of the network this is the most important technical issue for applying e-management.

E-business opens new areas of investment and spreads products and services all over the world. This creates the most important challenges, such as, expanded competition, increasing of customer power, rapid change which makes it hard to know when to “leap in” and invest, difficulty in establishing customer trust in a virtual world and cross border transactions/sales and territory agreements.

E-management security is the most serious challenge facing the organization. From many papers studied on the e-management security issue, there are many risks impacting the safety of the organizational environment in the daily work. These risks were affecting the companies in differing degrees, indicating the existence of a serious e-business security problem [15].

Conclusion

E-management success faces a lot of barriers and it has many challenges which need to be considered in order to succeed. The human factor plays a big role in e-management success and security. Although there are many benefits from applying e-management in an organization, there is still a lot of work that has to be done in order to establish a safe environment and protect the work going through the internet. Many studies should be done to understand the problems facing e-management in globally and in particular countries.

Furthermore, socio-cultural factors are among the most preventive obstacles in the application of e-management whereas technical and humanistic factors are amongst the least important ones [8]. It is obvious that cultural and organizational factors should be emphasized in order to resolve the obstacles. Development of cultural awareness to apply IT, enhancement of people’s and authorities ` awareness of the structure, performance and advantages of IT adoption and application, development of sufficient network and communication infrastructures, development of the application of e-services such as E-banking and e-insurance, motivating and training employees and managers for effective application of e-management are among the most important factors that should be noticed in order to improve the current situation of e-management.

References

[1] Dibrell, C. C., Miller, T. R. (2002.) Organization design: The continuing influence of information technology.

[2] Granville, B., Leonard, c., & Manning, J. (2001), Information technology and developing countries: potential and obstacles.

[3] Li, J., & Huang, J. (2004). An exploratory study of e-business success factors. Journal of electronic science and technology of China, 2(3), 167-172.

[4] Chaffey, D. (2011). E-Business& e-Commerce Management. Prentice Hall.

[5] Patrick C., Peter Raven, "Barriers to Effective E-Business in Developing Countries", International Business & Economics Research Journal, 1(4) 39.

[6] Peter Lord (2002), Managing E-Business Security, Challenges, oracle white paper

[7] Seresht, H. R., Fayyazi, M., &Asl, N. S. (2008). E-management: Barriers and challenges in Iran. E-OwerKraklead, Iran

[8] Narendra Kumar Tyagi, Srinivasan,S., (2001). Ten-Stage Security Management Strategy Model for the Impacts of 'Security Threats on E – Business', International Journal of Computer Applications, 21(5)

[9] Al-Malik, Bin Mohammed Bader, (2007) "Administrative and Security Dimensions of e-management in Saudi Banks."

[10] Jajodia, S. Noel, B. O'Berry, (2003), "Topological analysis of network attack vulnerability", in Managing Cyber Threats: Issues, Approaches and Challenges**,** V. Kumar, J.Srivastava, and A. Lazarevic (eds.), Springer, Germany.

[11] Bichler, M. (2001). The future of e-markets: multidimensional market mechanisms. Cambridge University Press.

[12] Umble Haft, (2003), Enterprise resource planning: implementation procedures and critical success factors, European Journal of Operational Research.

[13] Huff L; Wade M. (2000), Cases in Electronic Commerce, Boston: Irwin/ McGraw-Hill.

[14] Lichtenstein, Sharman (2001**),** Effective Management and Policy in e-Business Security, 14th Bled Electronic Commerce Conference, Bled, Slovenia.

[15] IBM. Ten Success Factors for E-Business, (2002) http://www-4.ibm.com/software/info/soul/st/guide.html.

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

PARALLEL COMPUTING WITH MPI / MPICH CLUSTER NETWORK

Al-Khulaidi Abdualmajed Ahmed.

Saba University, Sana'a Republic of Yemen

Article info

Article history: Accepted May, 2014

Keywords:

Message passing interface

Parallel computing

Parallel program

Abstract

The work aims to speed up the performance of processing wring parallel computing. Parallel computing is being used in many organizations using Open/Mpi. In our work we used Mpi/Mpich after modifying of using new algorithm to improve its performance. Real-time was measured computing the modified Mpi/Mpich and the advanced Mpi/Mpich

* Corresponding author: Dr. Al-Khulaidi Abdual majed Ahmed .
E-mail address: a.alkhulidi@sabauni.net

Introduction

Package MPI/MPICH has been used widely in the parallel computing .There are more than one package used to make the parallel computing such as Openmpi , cluster matic , MPI/MPICH,..etc. The best of packages in the MPI/MPICH, as it is easy to deal with programming language like C language in terms of connection [3].

Independence of Distributed Memory Processors

In computing systems with distributed memory, processors operate independently of each other. Parallel computations in such circumstances, must be able to distribute the computational load and organize interaction (data transmission) between processors [1].

Providing a data interface (message passing interface - MPI).

Under MPI which adopted a simpler approach, to solve this problem it is important to develop a program which should be the only program running at the same time on all available processors. To avoid identity calculations on different processors, we can, firstly, substitute different data for the program on different processors, and secondly, use available means in the MPI to identify the processor that runs the program, (thereby giving the opportunity to organize the differences in the calculations depending on the program of the processor).

Such a method of organization of parallel computing has the model name (single program multiple processes, SPMP). For the organization of information exchange between processors in the most minimal variant enough operations transmit and receive data (in this case, of course, there must be a technical possibility of communication between the processors - channels or communication lines). In MPI there are a whole set of data transfer operations.

Explaining Mpi and Mpich and Differentiated With Them

MPI is message passing interface and is used as directive while writing parallel programs in programming language. MPICH is a library including functions of parallel computing and is uploaded on computer. While writing parallel program, we must operate the library MPICH and we input the directive MPI in code program. Application parallel programs in local network, parallel program are applied on number of computer where each computer consists of more than one processor.

Ways of Data Transfer By Mpi In Parallel Computing In Cluster Network

They provide different ways of data transfer. That these features are the strong points of MPI (t in particular, testifies to the very name of MPI).

MPI would greatly alleviate the problem of portability of parallel programs among different computer systems - a parallel

program, developed in C or FORTRAN algorithm languages, using MPI library, as a rule, will run on different computing platforms.

MPI improves the efficiency of parallel computing, as it is now virtually every type of computer systems, there are libraries implementing MPI, to the maximum extent that they take into account the possibility of computer equipment.

MPI reduces, in some respects, the complexity of parallel program development, since, on the one hand, most of the considered methods of data transmission provide standard MPI, and on the other hand, already have a large number of libraries of parallel methods which were created by using MPI[3].

To explain what is meant by MPI? First, MPI - is a standard that must satisfy a means of organizing the transfer of messages. Secondly, MPI –is a software tool that enables transmission of messages that meet all the requirements of the standard MPI. Thus, according to the standard, these tools should be organized in a library of software functions (libraries MPI) and should be accessible to the most widely used algorithmic languages C and FORTRAN. Such «duality» MPI should be considered when using terminology. Typically, the acronym MPI is used when referring to the standard and a combination of «library MPI» indicates a particular software implementation of the standard. The notation used for MPI libraries MPI, and for the correct interpretation of the term should take into account the context.

Consider the number of concepts and definitions that are fundamental to the standard MPI.

Under a parallel program MPI there are set of concurrent processes. Processes can run on different processors, but a single processor can be located and some processes (in this case response can be implemented in time-sharing mode). In the limiting case for the execution of a parallel program can be used by one processor - as a rule, this method is used for initial validation of parallel programs.

Each process of a parallel program is generated based on a copy of the same software package (SPMP model). This code, presented in the form of an executable program, must be available at the time of running the parallel program on every processor. The source code for the executable program is developed on C or FORTRAN algorithms with some implementation of MPI library.

The number of processes and that of processors are determined at time of running a program by means of a parallel program executing MPI-programs. In the course of calculations these numbers cannot be changed without the use of special, but rarely personnel involved means that the dynamic generation of processes and management has appeared in the MPI standard version 2.0. All processes of the program are sequentially numbered from 0 to p-1, where p

is the total number of processes. The process number is called the rank of the process.

The implementation of MPICH allocates a specified number of processes among the available computing nodes without considering the constraints of available resources to them. Additionally, MPICH does not include information structure assignments and the heterogeneity of its component tasks, which leads to potential loss of productivity. Therefore, in computer clusters, MPICH uses such software, such as scheduler and resource managers. But here we must bear in mind that these applications are usually used for a wide range of tasks, and they cannot take into account the specific features of various problems arising from the solutions of the compound assignment.

We conclude that this package has a problem while comparing it with other packages such as absence of execution order control, resource allocation between processors, and status information task in the queue.

Conclusions

This package provide us with parallel computing in cluster network to increase the performance speed so we can do without a lot of processors, but this package has disadvantages such as absence of execution order control , resource allocation between processors , status information task in the queue.

References

[1] Hockney, R. W., & Jesshope, C. R. (1988). Parallel Computers 2: architecture, programming and algorithms (Vol. 2). CRC Press.

[2] Lifka, D. A. (1995, January). The anl/ibm sp scheduling system. In Job Scheduling Strategies for Parallel Processing (pp. 295-303). Springer Berlin Heidelberg.

[3] Ward Jr, W. A., Mahood, C. L., & West, J. E. (2002). Scheduling jobs on parallel systems using a relaxed backfill strategy. In Job Scheduling Strategies for Parallel Processing (88-102). Springer Berlin Heidelberg

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

PALXSS: CLIENT SIDE SECURE TOOL TO DETECT XSS ATTACKS

Tawfiq S. Barhoom *, Mohammed H. Abu Hamada

Islamic University Gaza, Palestinian Territory, Occupied

Article info

Article history: Accepted May ,2014

Keywords:

Cross-Site Scripting
Malicious script codes
Client side

Abstract

Cross-Site Scripting is one of the main attacks of many Web-based services. Since Web browsers support the execution of scripting commands embedded in the retrieved content, Attacker can gain this feature maliciously to violate the client security such as confidentiality. The public sites (i.e. social network) provide the attacker with ability to post there malicious code into a context which in the future to be shown to other participants. Detecting these malicious script codes is necessary for client side; the detection can be done by using detection tools used at client side. This paper describes the overall problem and elaborates on the possibilities to solve the problem with actions at client side to reduce the danger of Cross-Site Scripting attacks. In this work a new secure tool is developed using python language, which called PalXSS, two factors are used to evaluate it: performance and accuracy. The results show the accuracy of PalXSS tool is 90.24% which satisfies the users need compared with other tools.

* Corresponding author: Dr. Tawfiq S. Barhoom.
E-mail address: tbarhoom@iugaza.edu.ps

Introduction

Social networks, such as Facebook and MySpace, blogs and micro-blogs, such as Twitter, and other content providing services that are built on users' collaboration, such as YouTube and Flickr, are considered the killer applications of the last few years [1]. Also, everything has two sides. On the opposite side, these dynamic websites also provide a good platform for hackers to inject malicious code, as well. If the code is executed behind the web browser, it changes the web page according to the code automatically. Therefore, a lot of famous websites were injected with malicious code by hackers and a lot of visitors were attacked. Moreover, owing to the extensive spread of Web 2.0 and each user's blog can be shared with his/her friends as well. So, if one blog has been injected with malicious code, all the visitors of the blogger's friends will be infected and constantly infect their friends. Therefore, the speed of spreading is even quicker than previously. Eventually, the website provider will lose a lot of money and its reputation will be damaged, as well [2].

Cross-site scripting (XSS) attack method was first discussed in Computer Emergency Response Team (CERT) advisory back in 2000 [3]. But, even today cross-site scripting is one of the most common vulnerabilities in web applications; it has a widespread vulnerability in Web applications and was ranked first in OWASP Top Ten report 2007 and second in OWASP Top Ten report 2010 [4]. It happens as a result of data received from a malicious person and then sent to third parties. Systems that receive data from users and display it on other users' browsers are very vulnerable to an XSS attack. Wikis, forums, chats, web mail - are all good examples of applications most susceptible to XSS. This type of vulnerability allow hackers to inject the code into the output application of web page which will be sent to a visitor's web browser and then, the code which was injected will execute automatically or steal the sensitive information from the visits input. This code injection, which is similar to SQL Injection in Web Application Security,

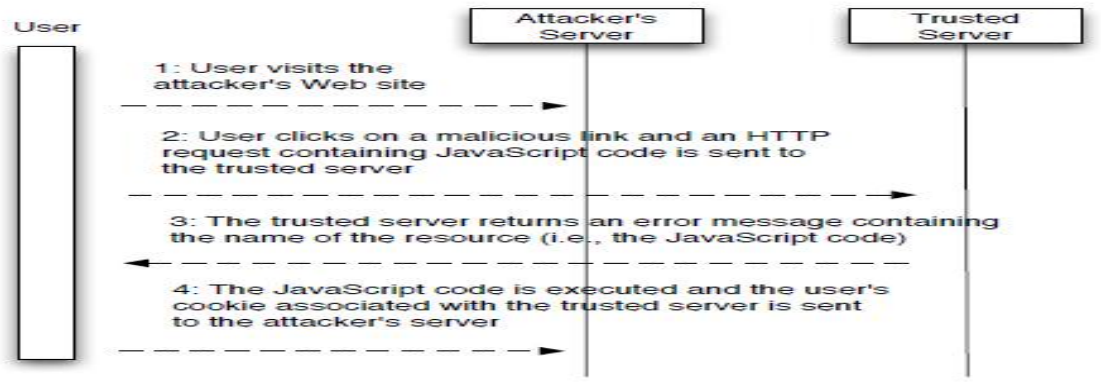

Fig.1. A typical cross-site scripting scenario [5].

can be used in three different ways namely "Persistent XSS", "Non-Persistent XSS" and "Dom- based XSS" Fig. 1. Vulnerabilities in Web applications can be discovered in various ways. In the black-box approach the Web Vulnerability Scanner has no knowledge about internal operation and operates only on the interfaces that can be accessed from the outside. The internals of the application are kept secret, source code cannot be accessed and most of the time, the Web Vulnerability Scanner doesn't even know which type of Web server the application runs on. All information about the Web application must be gathered with the help of tools such as Web Vulnerability Scanners or manually by inspecting the HTTP responses and by trying different input values to understand the behavior of the Web application [6]. In white-box testing [6], the opposite is true. The Web Vulnerability Scanner has access to the internal workings of the Web application and every request can be traced. All necessary information is then available and can even access the source code to find vulnerabilities. The internal mechanisms of the Web application can be traced in detail using debugging tools.

In the scope of this work, only black-box techniques are investigated as black-box testing is typically the case for most Web Vulnerability Scanners testers and also for attackers with malicious intent. To find the vulnerability, python language was used which is simple language, an easy to learn, powerful programming language and free and open source language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant syntax and dynamic typing, together with its interpreted nature, make it an ideal language for scripting and rapid application development in many areas on most platforms [7].

Related Works

There are largely two distinct countermeasures for XSS prevention at server side: Input filtering and output sanitation. Input filtering describes the process of validating all incoming data. The protection approach implemented by these filters relies on removing predefined keywords, such as <script, JavaScript, or document. Output sanitation is employed, certain characters, such as <, ", or ', are HTML encoded before user-supplied data is inserted into the outgoing HTML. As long as all untrusted data is "disarmed" this way, XSS can be prevented. Both of the above protections are known to frequently fail [8], either through erroneous implementation, or because they are not applied to the complete set of user-supplied data. Client side solution acts as a web proxy to mitigate Cross Site Scripting attack which

manually generates rules to mitigate Cross Site Scripting attempts. Client side solution effectively protect against information leakage from the user's environment. However, none of the solutions satisfy the need of the client side. There are several client-side solutions.

Hallaraker et al. [9] proposed a strictly client-side mechanism for detecting malicious JavaScript's. The system uses an auditing system in the Mozilla Firefox web browser that can perform both anomaly or misuse detection. This system monitors the execution of JavaScript and compares it to high level policies to detect malicious behavior. This solution is insufficient because if new vulnerabilities should be detected, new rules have to be implemented and the browser has to be rebuilt. Also it is possible to detect various kinds of malicious scripts, not only XSS attacks. However, for each type of attack a signature must be crafted, meaning that the system is defeated by original attacks not anticipated by the signature authors. Some authors [10-14] have proposed the use of static analysis techniques to discover input validation flaws in a web application; however, this approach requires access to the source code of the application [10, 11]. Moreover, those static analysis schemas are usually complemented by the use of dynamic analysis techniques. Huang et al [12], Balzarotti et al [14] used this techniques to confirm potential vulnerabilities detected during the static analysis by watching the behavior of the application at runtime. Several existing systems have been adapted to detect XSS. Application level firewalls [5], reversal proxies [15] and IDS (Intrusion detection systems) [16, 17], have been adapted to try to mitigate the XSS problem. Firewalls focus on tracking sensitive information and controlling whenever data is to be sent to untrusted domains. Reverse proxies receive all responses from the web application and check whether there are any unauthorized scripts on them. IDS approaches deal with the identification of traffic patterns that allow the detection of known XSS attacks.

Kirda et al [5] presented Noxes as a client-side Web-proxy that relays all Web traffic and serves as an application-level firewall. The main contribution of Noxes is that it is the first client-side solution that provides XSS protection without relying on the web application providers. Noxes supports an XSS mitigation mode that significantly reduces the number of connection alert prompts while at the same time providing protection against XSS attacks where the attackers may target sensitive information such as cookies and session IDs. The approach works without attack-specific signatures. The main problem of Noxes as that it requires user-specific configuration (firewall rules), as well as user interaction when a suspicious event occurs.

Another client-side approach was presented by Vogt et al [13], which aims to identify

information leakage using tainting of input data in the browser. The solution presented in this paper stops XSS attacks on the client side by tracking the flow of sensitive information inside the web browser. If sensitive information is about to be transferred to a third party, the user can decide if this should be permitted or not. As a result, the user has an additional protection layer when surfing the web, without solely depending on the security of the web application.

Gal´an et al [18] completed the scope of vulnerability scanners by allowing them to check the presence of stored–XSS vulnerabilities in web applications. The system proposed was based on multi–agent architecture allowing for each one of those tasks to be carried out by a different type of agent. This design decision has been taken to allow each of the stages of the scanning process to be performed concurrently with the other stages. It also allows for the different subtasks of the scanning process to take place in a distributed and/or parallel way. The agent that explores the web site in order to find the injection points where stored–XSS attacks could be launched. This parsing process is similar to that of web crawlers and spiders. XSS-Me the One of the best open source tools was the Exploit-Me series presented by securitycompass.com [19]. Security Compass created these tools to help developers easily identify cross site scripting (XSS) and SQL injection vulnerabilities.

XSS-Me is a Firefox add-on that loads in the sidebar. It identifies all the input fields on a page and iterates through a user provided list of XSS strings: opening new tabs and checking the results. When this process completes you get a report of what attacks got through, what didn't, and what might have. The tool does not attempt to compromise the security of the given system. It looks for possible entry points for an attack against the system. There is no port scanning, packet sniffing, password hacking or firewall attacks done by the tool. You can think of the work done by the tool as the same as the manual testers for the site manually entering all of these strings into the form fields. This tool is good for detecting XSS attacks but it needs user interaction to do testing (like manual testing), moreover its cannot follow all links in the website, as a result, it scans the link provided by the user click.

All client-side solutions share one drawback: the necessity to install updates or additional components needed on each user's workstation. While this might be a realistic precondition for skilled, security-aware computer users, it is perceived as an obstacle or is not even considered by the vast majority of users. Thus, the level of protection such a system can offer is severely limited in practice.

Methodology

Current fully automated Web Vulnerability Scanners (WVS) has three major components: A crawling component, an attack component and an analysis component [20]:

*1. **Crawling Component**:*

The crawling component collects all pages of a Web application. It uses an input URL as seed starts following links on each page and store the result in list. The crawling module is arguably the most important part of a Web application Vulnerability Scanner; if the scanner's attack engine is poor, it might miss vulnerability, but if it's crawling engine is poor, then it will surely miss the vulnerability [21].

2. Attack Component:

The attack component scans website, extracts all internal links then scans all crawled pages forms field which are used in URL parameters then injects various attack patterns into these parameters; Parameters can be part of the URL query string or part of the request body in HTTP POST requests. Both are equally exploitable. In this work, most examples have forms with input fields to illustrate vulnerable parameters [20].

3. Analysis Component:

The analysis component parses and interprets the server's responses. It uses attack-specific criteria and keywords to determine if an attack was successful. An attack vector is a piece of HTML or JavaScript code that is added into a parameter in-order to be reflected to users by being embedded into a HTTP response. The goal of an attack vector is to make user browser execute malicious code. The malicious code can be either fetched from trusted website or be part of the attack vector itself, although the former allows more complex exploits. two examples for typical attack vectors are:

1. <script src="http://attacker.com/exploit.js"></script>

loads and executes a remote script from website.

2. <body onload="document.write('<img src=http://attacker.com/?'+document.cookie+'/ >')">

performs cookie stealing as part of the attack vector.

Our proposed model architecture is shown in fig. 2. In step 1, all pages are crawled and stored into the list (step 2). For simplicity and easy installation, data is stored in a text file rather than in a database. Stores are only small amounts of data (a few kilobytes) that don't cost much performance. In step 3, the attack module takes pages from the list with modifiable parameters, injects attack vectors and passes the responses to the analyzer, which analyzes them for injected patterns in step 4. In this step, the attack component injects a

common attack vector such as <script>alert (“XSS”) </script> and the analysis component uses a regular expression to search for the very same injection string. If the attack pattern is found unmodified (no characters were added or replaced), the attacked parameter is vulnerable to XSS.

PalXSS tool are used to detect XSS attack by performing an attack and checking the resulting page if the malicious code is injected without modification. The steps are:

1. A selection of attack vectors is obtained from an attack vector repository; XSS attack vectors are commonly stored in repositories and include the description of the attack as well as the script code to be injected.

2. Selected attack vectors are launched against inputs of the web application. Those attack vectors are generally injected in an

HTTP request as parameters or as fields in a web form.

3. PalXSS tool receives the responses to the requests containing the injected code.

4. The PalXSS tool checks for the presence of injected script in the received responses. If affirmative, XSS attack is considered successful and a vulnerability of the scanned web application has been discovered.

Implementation

PalXSS is a secure tool which is written in python language. The tool consists of four main classes; these classes are:

1. ***Web Page Parser class:***

When the client launches this class, python script will prompt him to enter a URL. The script will connect to the URL entered and hunt for any <a href> elements, as it systematically retrieves information from the pages it visits and it propagates through the site following the hyper-links it finds. Nevertheless, it differs from the typical web crawler in two aspects: (1) It just follows the hyper-links with destination to the scanned site discarding all external links and, (2) the information recovered are web forms

2. ***Spider Class:***

In this class, the script will connect to the URL entered in the previous step and hunt for any <form> elements. It will output the attributes associated with the elements allowing client to see what method is being used and what action is being performed. Once all the <form> elements are collected, it will then move on to <input> tags. All entries found will then be displayed as "possible" targets.

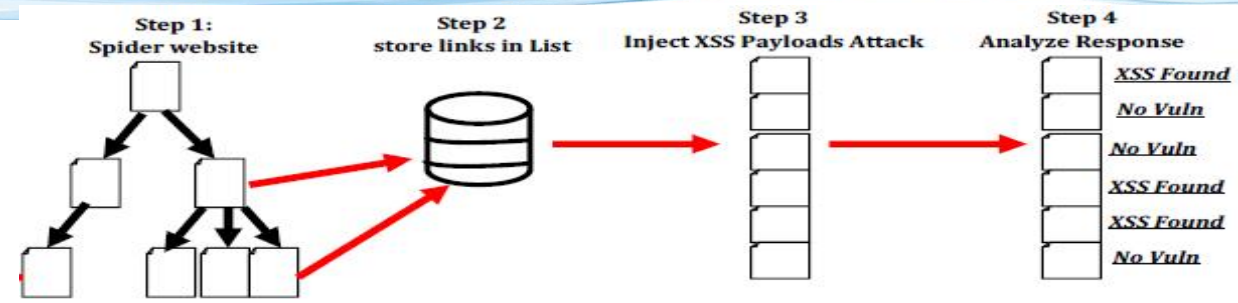

Fig 2: Proposed model architecture

3. *Script Injector Class:*

This class extracts the collection of web forms elaborated by the web page parser class and register in the injection repository. The class will inject a collection of XSS attack vectors from a well-known repository into different input fields of each of the injection points

4. *The Store Class:*

This class shows the report which contains: the links extracted from the base URL, and the input form field hacked. This report helps the client to know the XSS vulnerable in the website.

Dataset

We performed a series of experiments with our prototype implementation to demonstrate its ability to detect previously known cross-site scripting vulnerabilities, as well as new ones. To this end, PalXSS was run on seven popular XSS Payloads. The dataset of attacks used for evaluation our tool were extracted from a repository of XSS attack vectors found in http://ha.ckers.org/xss.html. Those vectors use different ways of inserting arbitrary script code trying to be unnoticed by the web application and, in our case, to be incorporated as legitimate content in the web application. As the attack vectors in the repository are large, the experiment tests every type to define the code accepted. The XSS payloads show the code accepted by testing our tool in real websites. The number of injection attacks can affect the performance of detection. To enhance the performance, we took seven attacks as default in our tool that was accepted in most of the tests.

Evaluation

This section presents the evaluation of PalXSS tool. The task was to detect all XSS vulnerabilities in online website. Different categories of tests were conducted to ensure that our solution works. The two major aspects of the evaluation application are (i) to compare our work architecture with the traditional architecture of scanners and (ii) the comparison of the execution time and accuracy by three tools.

An implementation of the proposed system was developed with the purpose of testing and evaluating the scanner against different websites; three scanners were used for the evaluation. These scanners work at the same condition with the same parameters; also these tools share the same methodology. The tools are:

Acunetix 7, XSSploit: and PalXSS. Fig. 3 shows the execution time of our tool compared to other tools e.g., the first website of testing is http: xss.progphp.com; the execution time of our tool is 84/sec, it has a better performance compared to XSSploit tool, while it has law performance when compared to Acunetix tool.

The execution time of our tool is the minimum in all cases than other tools, while in some cases such as in website 8 as shown in fig. 3 the execution time is the maximum, this result occurs because the number of field detected in this site is ten which takes more time to check the result than other tools which can't detect them, this gives the best accuracy.

The result in the table 1 shows the accuracy of PalXSS tool as the best compared to other tools; the average detection rate of PalXSS tool even 90.24%, while the average detection rate of XSSploit was 24.39% and the average detection rate of Acunetix tool was 57.32%.

The accuracy of PalXSS tool can be satisfying the users to use this tool among others.

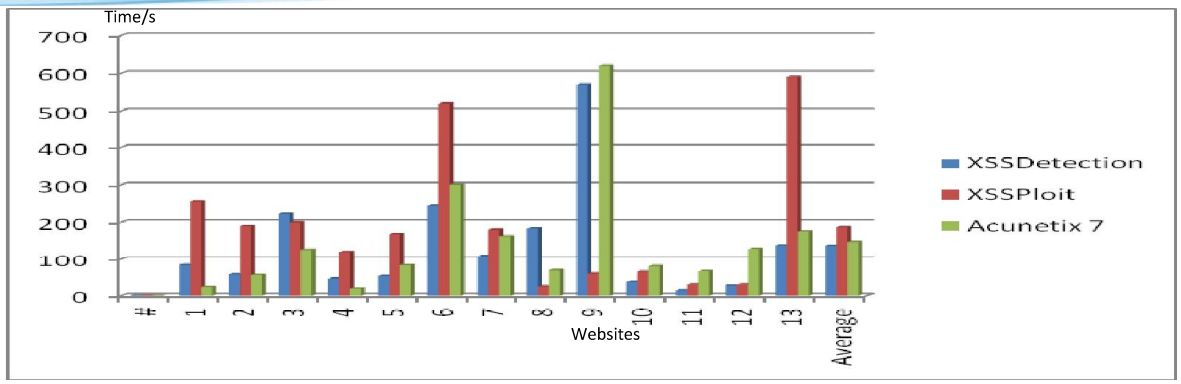

Fig.3. Comparison of three tools in this works

#	Websites	Vuln. Filed	Pal XSS	XSS Sploit	Acunetix
			Vulnerable field Detected		
1	http://xss.progphp.com	2	2	2	2
2	http://testasp.vulnweb.com	1	1	1	1
3	http://demo.testfire.net	2	1	2	2
4	http://www.kaspersky.com.pt/base/guest/mimemessage/test_multibyte_message.php	6	6	0	0
5	http://testphp.vulnweb.com	2	0	2	2
6	http://demo.arcticissuetracker.com	2	1	0	2
7	http://zero.webappsecurity.com	5	1	5	5
8	http://www.binaryanalysis.org/en/home	10	10	1	6
9	http://www.socialweb.net/Accounts/general.lasso?new=1	25	25	0	10
10	http://www.qou.edu/contactUs.do?key=2	6	6	5	2
11	http://www.maktoobblog.com/search	1	1	1	1
12	http://www.gametiger.net	5	5	1	5
13	http://www.asianave.com/user/register.html	15	15	0	9
Total		82	74	20	47
Average			**90.24%**	**24.39 %**	**57.31%**

Table 1: the detection rate of three tools

Recommendations

We recommend that the regular security tests need to be part of an effective software development process; furthermore, detected tool must play an important role in providing a testing framework. The developers must train well enough about the security holes in the website. Security awareness and education is incorporated throughout several stages such as creating documentation, threat modeling etc. Nevertheless, it is important to understand that the goal of vulnerability scanning is to reveal security flaws so that developers can trace these issues and implement security mechanisms. In addition, we propose that as our culture becomes more dependent on information, social engineering will remain the greatest threat to any security system. Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate.

Conclusion

This paper analyzed the problems that current Web Vulnerability Scanners are facing when trying to detect XSS vulnerabilities, as reported in recent research it was found that the vulnerability scanners are a promising mechanism to fight the XSS vulnerabilities in web applications. One reason for the widespread of XSS vulnerabilities is that many developers aren't trained well enough. Current proposals allow to automatically identifying that kind of security holes, although they also present an important limitation: the accuracy of detecting can't satisfy the users need and the performance is low. In this work, a secure tool was developed which called PalXSS; this tool works in forum, takes input form field as a target to detect XSS attacks by injecting malicious JavaScript code.

Two factors were used to evaluate the new tool: the performance and accuracy. The average detection rate of PalXSS tool is 90.24% while the Acunetix is 57.31% and XSSploit is 24.39% in order. The results show the accuracy of PalXSS tool satisfying the users need than other tools. In addition, the execution time of the PalXSS tool had 137/sec, while the Acunetix and XSSploit had 147/sec,187/sec in order; this result shows that the performance of our tool have high performance and accuracy among other tools used in this work. The detection rate of PalXSS tool can satisfy the client's need, which gives the motivation to enhance the tool in the future work.

References

[1] Athanasopoulos, E. (2011). Modern Techniques for the Detection and Prevention of Web2. 0 Attacks (Doctoral dissertation, University of Crete)..

[2] B. Almurrani "Cross-Site-Scripting (XSS) Attacking and Defending" BACHELOR´S THESIS, ABSTRACT TURKU UNIVERSITY OF APPLIED SCIENCES Degree Program in Information Technology, Autumn 2009

[3] Cert advisory ca-2000-02 "malicious html tags embedded in client web requests. February 2000.

[4] Open Web Application Security Project. OWASP Web Application Scanner Specification Project. http://www.owasp.org/index.php/Category: OWASP Web Application Scanner Specification Project, 2010. [Online; retrieved June 19, 2010].

[5] Kirda, E., Kruegel, C., Vigna, G., & Jovanovic, N. (2006, April). Noxes: a client-side solution for mitigating cross-site scripting attacks. In Proceedings of the 2006 ACM symposium on Applied computing (pp. 330-337). ACM..

[6] Doupé, A., Cova, M., & Vigna, G. (2010). Why Johnny can't pentest: An analysis of black-box web vulnerability scanners. In Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 111-131). Springer Berlin Heidelberg..

[7] Guido van Rossum Fred L. Drake, Jr., editor " Python Tutorial Release 2.3.3 "December 19, 2003.

[8] S. Christey and R. Martin, "Vulnerability type distributions in cve", version 1.1. [online], http://cwe.mitre. org/documents/vuln-trends/index.html, (09/11/07), May 2007.

[9] Hallaraker, O., & Vigna, G. (2005, June). Detecting malicious javascript code in mozilla. In Engineering of Complex Computer Systems, 2005. ICECCS 2005. Proceedings. 10th IEEE International Conference on (pp. 85-94). IEEE..

[10] Wassermann, G., & Su, Z. (2008, May). Static detection of cross-site scripting vulnerabilities. In Software Engineering, 2008. ICSE'08. ACM/IEEE 30th International Conference on (pp. 171-180). IEEE.

[11] Jovanovic, N., Kruegel, C., & Kirda, E. (2006, May). Pixy: A static analysis tool for detecting web application vulnerabilities. In Security and Privacy, 2006 IEEE Symposium on (pp. 6-pp). IEEE.

[12] Huang, Y. W., Yu, F., Hang, C., Tsai, C. H., Lee, D. T., & Kuo, S. Y. (2004, May). Securing web application code by static analysis and runtime protection. In Proceedings of the 13th international conference on World Wide Web (pp. 40-52). ACM.

[13] Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007, February). Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. In NDSS.

[14] Balzarotti, D., Cova, M., Felmetsger, V., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2008, May). Saner: Composing static and dynamic analysis to validate sanitization in web applications. In Security and Privacy, 2008. SP 2008. IEEE Symposium on (pp. 387-401). IEEE.

[15] P. Wurzinger, C. Platzer, C. Ludl, E. Kirda, and C. Kruegel. Swap: " Mitigating xss attacks using a reverse proxy". In Proceedings of the ICSE Workshop on Software Engineering for Secure Systems (SESS '09), 2009.

[16] C. Kruegel and G. Vigna. " Anomaly detection of web-based attacks". In Proceedings of the 10th ACM conference on Computer and communications security, pages 251–261. ACM New York, NY, USA, 2003.

[17] M. Johns, B. Engelmann, and J. Posegga. " Xssds: Serverside detection of cross-site scripting attacks". In Proceedings of the Annual Computer Security Applications Conference, pages 335–344. IEEE Computer Society Washington, DC, USA, 2008.

[18] E. Gal´an, A. Alcaide, A. Orfila, J. Blasco "A Multi–agent Scanner to Detect

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

CLOUD COMPUTING ADOPTION: BRAND EQUITY IMPACT ON USERS' CHOICE

Emad Abu-Shanab *, Huda Qasem

Yarmouk University, Jordan

Article info

Article history: Accepted June, 2014

Keywords:

Cloud computing
Security
Brand reputation

Abstract

Cloud computing is becoming a strategic choice for organizations and individuals offering great facilitations for startup organizations with cost reduction and flexible and handy scalability. But with the many advantages associated with the adoption of cloud computing, the environment suffers from many risks like: security, privacy, trust issues, and lack of standards. Still some large venders are emerging with many concerns in relation to data residing on others' servers. This paper will explore the cloud computing environment, its risks, and the factors influencing its adoption. Finally, a proposed framework is depicted and empirically tested to estimate the associations between intentions to use cloud computing and the following factors: security, privacy, prior online experience, vender's brand reputation, trust in the brand name, and brand equity. Results indicated a significant prediction of trust in the brand by experience and brand reputation. Also, trust significantly predicted brand equity, and brand equity significantly predicted intention to use the cloud service. Results and conclusions are discussed at the end of paper.

* Corresponding author: Dr. Emad Abu-Shanab.
E-mail address: abushanab@yu.edu.jo

Introduction

In the so called digital age, experts predicted the end of brand management all together; these predictions are far from being accurate. Not only brand management still exists, but so many digital brands have risen. Some companies even created great brand equity such as yahoo, Facebook and Google that put them ahead of a number of the most established traditional off-line brands.

Despite the claims that Internet can erode brand power due to many emergent business models like name your price, and price comparison sites, or simply the accessibility of vendors online, brand equity continues to impact users behavior, purchasing decisions, and adoption intentions [42].

In the past, IT was considered an organizational asset; like money, time and labor. Today, things are changing. The financial crisis left companies with less money that they went to utilize an IT infrastructure through outsourcing. Businesses no longer need to acquire, and maintain an IT infrastructure. Businesses can benefit from the concept of cloud computing [39].

Despite its great potential, cloud computing faces significant issues; the mere idea of entrusting your data to another company sounds dangerous to many people [32]. Ignoring the high risks embedded within this path seem unrealistic [14]. Security challenges, and the ability to sustain an acceptable level of data integrity and privacy as data storage is outsourced, are few of many challenges that face this emerging technology [29].

With the continuous growth in cloud computing, which will become a 19.5B business by the year 2016 [10], many brand names in the technology sector are competing for a higher market share [36]. Such issue makes it extremely necessary to study the aspects that make a user choose one vendor over the other, and how much of their choice depended on the venders brand equity.

Information based industries, such as cloud computing technology, are the most affected by the digital revolution. The Internet is not just another channel, it's the only channel. Such industry is dependent on the first impression they make on a user, and the way they greet a returning customer are all critical factors for the survival in the information industry. The online branding game is on and they have to win [43]. This paper will explore the literature related to cloud computing and the influence of brand equity on the intention to use cloud computing. The factors influencing brand equity will be explored. An empirical test will be conducted to estimate the research model. Finally, conclusions and future work will be depicted.

Literature Review

Introduction to Cloud Computing

Cloud computing is commonly used by various users as they can easily connect using web service or web browsers. CC is characterized by its dynamic infrastructures, global access, massive scalability, fine grain pricing, standard platforms, and management services. Cloud computing is defined as *"an information technology-based business model, provided as a service over the Internet, where both hardware and software computing services are delivered on-demand to customers in a self-service fashion, independent of device and location within high levels of quality, in a dynamically scalable, rapidly provisioned, shared and virtualized way and with minimal service provider interaction"* [25].

Other researchers defined cloud computing as a convenient model that allows for ubiquitous, on-demand network access to a sharable pool of computing resources (e.g., networks, servers, storage, applications, and services) that can be easily used with minimal management effort or vendors interaction [28]. It's a term used to refer to accessing resources (software applications, storage, and processing power) over the Internet, it has helped businesses to improve capabilities and add capacity without the need to install new software, train employees to use it, and worry about its maintenance [23].

There are four service models for cloud computing [50] [21] [26] [22]:

1. *Software as a Service (SaaS):* which offers an application as a service on Interne; making collaborate access of software and data easier than ever, where organizations or individuals pay per use.
2. *Platform as a Service (PaaS):* Used by developers for developing new applications. Allow them to launching new application for minimal expenses.
3. *Infrastructure as a Service (IaaS):* Providers Provide the features on demand utility, organizations pay fraction of the cost on the contrary to acquiring the infrastructure, small portions of cloud are provided for free (Sharon, 2012).
4. *Desktop as a service (DaaS):* Virtual Desktop Infrastructure where a third party can host desktop services, data storage, security and backup managed by service provider.

Another typology of cloud computing is distilled from the literature where four deployment models were proposed. The models depended on the status of organization and the cloud use [28][37] [46]:

- *Private cloud:* The cloud infrastructure is only dedicated to a single organization use or its business units, where the cloud is not open for public use. This type of cloud may be owned

by the organization itself or operated and managed by a third party.

- *Community cloud:* The cloud infrastructure is dedicated for the use of a specific community of consumers of a particular organization that have high security standards compliance considerations. Similar to the private cloud community, clouds can be managed and operated by the organization itself or a third party or somewhere in between.
- *Public cloud:* The cloud infrastructure is open for the use by the general public, business, and academic institutions. Also, organizations or governments may own, manage and operate this type of cloud, or some combination of the previous ones.
- *Hybrid cloud:* This cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community, or public).

The main characteristics of cloud computing are the following:

1) *scalability of infrastructure;* new capabilities can be added or dropped on need bases without the need to set up and modify infrastructure or set up new applications. 2) *Broad network access:* network availability and network access, with standard mechanisms through the heterogeneous platforms (e.g., mobile phones, laptops, and PDAs). 3) *Location independence:* clouds are location independent in some sense; there is practically no importance what so ever to the vendor's location. 4) *Reliability:* reliability is improved with the use of redundant sites, which makes cloud computing suitable for business continuity and disaster recovery. Finally, 5) *Economies and cost effectiveness:* Clouds regardless of the deployment model are much cheaper [50].

The previous review tried to explore the environment of cloud computing. The option of adopting cloud computing is not an easy one; it involves huge risks, but still provides substantial benefits and synergies. Fig.1 depicts a proposition by [38] that relates the type of business (institution) to the cloud computing deployment model. The framework is named Cloud Computing Business-Deployment Fit Model.

Type of Institution	Cloud Computing Deployment Model		
	Private	Hybrid	Public
Governmental Institutions	✓	✓	☒
Financial Institutions	✓	✓	☒
Small/Medium-Size Businesses	☒	✓	✓

Fig. 1: Cloud Computing Business-Deployment Fit Model

(Source: [38])

Based on the reviewed literature, it's safe to conclude that governmental institutions (with greater concerns as to where the service provider's jurisdiction) are most likely to create their own private cloud. Such option allows for better control, better security, and more reliance. An example case is the government of Japan which announced that by the year 2015 the country will have a private cloud that consolidates all governments IT systems, for better efficiency and less cost [12].

As for financial institutions, the idea of cloud computing seems to defy the principles on which theses institutions where founded. Due to the flexibility, high scalability and the low cost made possible by the cloud technology, banks and other financial institutions are easing their way to a new era of business. They are very much like governmental institutions and pretty much for the same reasons; financial institutions are most likely to adopt single tenant private cloud deployment model [15].

For better exploitation of this technology, both governmental and financial institutions may use public clouds for non-core activities in a hybrid cloud deployment model [12] [15].

While public clouds are less demanding in terms of cost (with using the pay as you go payment model), the freedom of service for businesses, and the management services offered by the service providers, make public clouds well suited for small and medium size businesses [33].

Online brand equity

The online environment has changed the branding game dramatically; a brand reputation in the online world has to be created, protected, and managed. Branding is one of the most important assets for any online vendor, if you are not searchable, if no one is talking about you, then you simply don't exist [19].

Users of information systems are most likely to experience some sort of anxiety as they chose

to store their information on a cloud. Such concerns may result from several risks associated with cloud computing, multi-tenancy [18][23] security and privacy [49][48]. These concerns are often referred to as perceived risk which is defined in literature as the nature and amount of concern the client may experience before making the decision to purchase a product or a service. Such concerns may result from inherited factors of the product itself, the place of purchase, mode of purchase, and product producer or service provider brand [11].

Brand equity is a source of reassurance for the customer in tangible goods, but it's equally important to the customer as he/she purchase an intangible service [8]. Given the fact that services provided through the Internet such as cloud computing services pose higher privacy and security threats to the user, increasing his/her perceived risk, and limiting their willingness to use those services, the desire to trust the vendor becomes even of greater importance.

Sources of trust in online brands

The literature is full of work related to trust in online services and brands. Research indicated a significant correlation between trust the intention to use a service or buy a brand in Jordan [3][4]. The following are the major factors influencing such level of trust.

Security and privacy: the more the user feels confident that his information is safe, the higher he trusts the website [6]. Users often look for clear privacy policies, because when the user find it easier to disclose personal information, that he wouldn't have disclosed otherwise [30] and therefore seen as a competitive advantage [6]

Word of the mouth: word of the mouth has repeatedly proven to be a powerful marketing tool. For a potential user to hear a good word on a vendor, would decrease the perceived risk and result in a higher level of trust, which in turn leads to higher intention to use or buy the brand [6] Word of the mouth often given in a form of advice is a major source of trust [7] this is usually due to the fact that users often trust their acquaintances more than they trust advertizing campaigns, it should be noted though that customers feel inclined to share their negative experience with other (negative word of mouth). So it is crucial that vendors try to meet customers' demands, listen attentively to their complaints and try to resolve them [30].

Vendor's reputation: vender's reputation is defined as the common perception of the brand held by most customers [30]. Better brand reputation means more online trust [16] [44] [6]. There for it isn't only important to build a good reputation online, but also to maintain such reputation, otherwise the vendor will end up losing customers [30]. Online experience: a good online experience has the power of further strengthening brand trust [6] , some of the most influential ways to improve users experience are using simple easy to understand

language, building a functional responsive site [44].

The Research Model and Hypotheses

In this study, our focus revolves around brand equity, which is a major factor in determining the intention to use a brand or buy from it. Our previous review and the understanding of the interactions of the previously mentioned constructs reflect a research model that is depicted in Fig .2. The major research questions to be answered in this work are the following:

RQ1: What are the factors influencing brand equity

RQ2: How far does brand equity shape customers intention to use the cloud.

Directly linked to the concept of perceived risk is trust; more trust in a particular brand has the power of decreasing the concerns consumers may experience regarding security or privacy [13] [34] [45]. More trust in a brand name is even more important than computer mediated environment and it has a great importance in creating brand equity [42]. When users and organizations work with cloud computing, security and privacy become important as data and information will reside on another party's server [48]. The privacy, security and trust association is of great value to the vendor, it's the reasons customer will accept the perceived risk and purchase the offered service,[27]. Privacy and security are important predictors of trust; they are explored much in research related to the services offered via the Internet. Users tend to favor vendors who guarantee their information security [9] as well as those who address their privacy concerns [17]. In a large scale study on the role of online trust in different websites, it was concluded that privacy and security are always relevant, and are of higher relevance when the risk of information preach are high [7] as any preach has the power to erode brand trust [43].

Based on the previous discussion, and taking into consideration the importance of privacy and security, the following hypotheses are stated:

H1: Information security is positively related to trust in the cloud

H2: information privacy is positively related to trust in the cloud

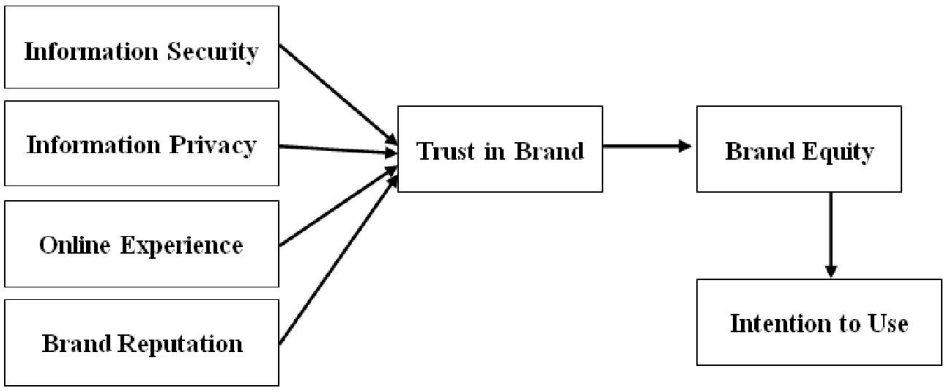

Fig. 2: The proposed research model

Any firm gains its reputation through the quality of the goods/services it offers and mainly customers prior experience and its credibility [40]. Brand reputation is also important in the online ever dynamic environment. Brand reputation is highly associated with trust [13] it is even suggested that vendor's reputation is more important to the customer than the value expected form the purchase itself [45]. Repeatedly by several studies, online experience also has significantly influenced trust in the brand [17] [44] [6]. Former experience with the vendor is a significant source of brand trust and a predictor of future use [30].

Based on that, the following hypotheses, related to customer's experience and vender's reputation, are stated:

H3: Customers' online experience is positively related to trust in the cloud

H4: Brand reputation is positively related to trust in the cloud

Trust has been seen as a driver of brand equity, a crucial factor in online environment [1] [5] [42], especially in the information based service environment that is highly associated with technological innovation where good branding is key to holding the customer attention[31]. Reestablished brand familiarity may decrease the perceived risk and thus improve the chances of adoption [32]. Some even suggest that the whole idea of brand equity is a surrogate for trust [20]

H5: Trust in the cloud is positively related to brand equity

Presumably, and based on [11] definition, brand name has an impact on our buying choices, where brand equity (brand awareness & brand meaning) impcats consumers behavior [8]. Also, since there is a greater inherited risk associated with cloud computing that gives even a greater weight to the brand equity, we propose the final hypothesis:

H6: Brand equity will positively influence the intention to use the cloud.

Data Analysis and Discussion

To test the research model and the hypotheses, we tried to target more professional

respondents through an online posted survey. The survey was posted on Google website and the link was sent to few e-mail lists and posted on a Facebook page. The survey items used were extracted from previous research and as shown in Appendix A at the end of paper. The model utilized 3 items for measuring information security, 3 items for information privacy, 3 items for brand reputation, 5 items for previous online experience, 4 items for trust in the brand, 3 items for brand equity, and 5 items for intention to use cloud computing (ITU). One of the items was deleted for redundant statement posted on the web (item 16). The sample reached in 48 hours 120, where we started analyzing the data. The demographics of sample are shown in Table 1.

It is obvious that the majority of sample holds a bachelor degree, and within the 20-40 years of age. Females are more than males, and missing values is not an issue.

To test the research hypotheses a structural equation modeling (SEM) analysis utilizing SmartPLS software and algorithms was conducted. A partial least squares SEM (PLS-SEM) does not assume normality but relies on a nonparametric bootstrap procedure to test the model.

In this procedure many smaller subsamples are drawn from the study sample and tested to reach the best model fit. The SmartPLS tool is free for academic purposes and calculates easily the item loadings and the correlations (path coefficients for the whole model are depicted). The results of the model estimation are shown in Fig. 3.

Table 1: Sample demographics

Gender	Count	%
Male	42	35.0%
Female	77	64.2%
Not reported	1	0.8%
Total	120	100%
Age	Count	%
Less than 20 years	6	5%
21-40 years	93	77.5%
41-60 years	19	15.8%
More than 60 years	0	0%
Not reported	2	1.7%
Total	120	100%
Education	Count	%
High School or less	11	0.2%
Bachelor	63	52.5%
Master/PhD	41	34.2%
Other	4	3.3%
Not reported	1	0.8%
Total	120	100%

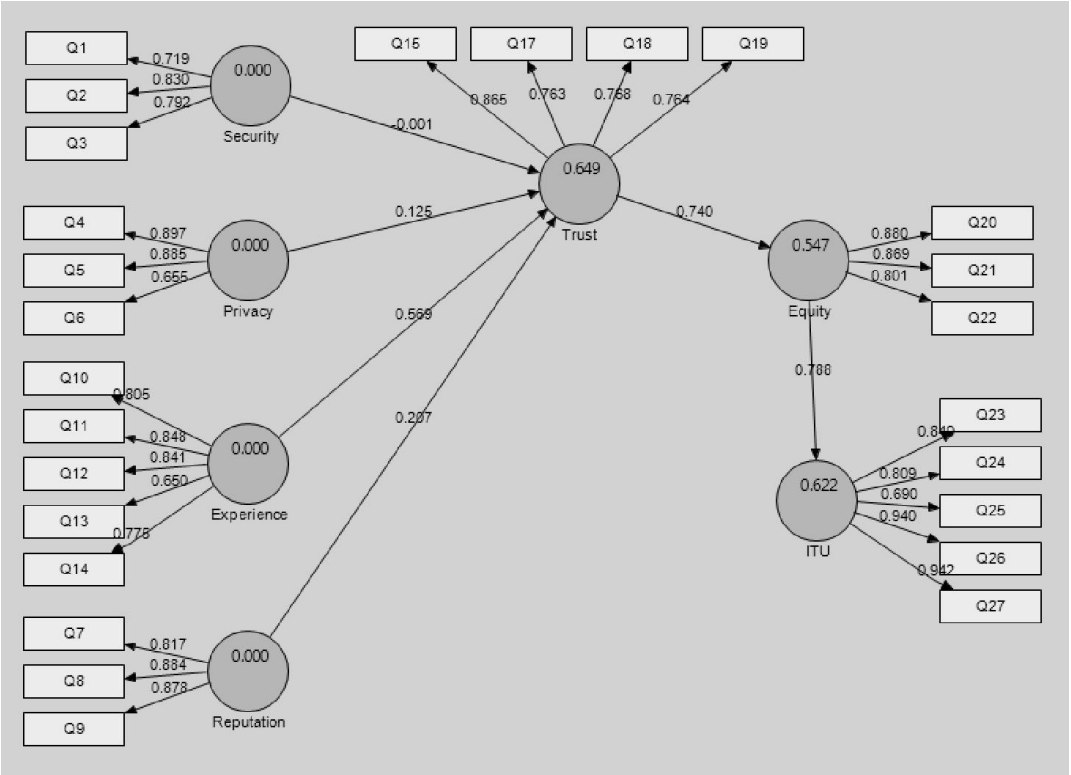

Fig. 3: The measurement model with path coefficients and factor loadings
The model is estimated using SmartPLS (Ringle et al., 2005)

The research model assumed a mediation effect of trust in brand and brand equity between the four independent variables and the ultimate dependent variable (ITU). Such issue is a test of the sequential building of influence of such domain, where we assume that security, privacy, experience and brand reputation all will have a significant influence on trusting a cloud computing website. Such argument will build into the brand equity and then users will use the service.

Results of the structural model indicated a good reliable set of measures (values on arrows between items and major variables. The values of loading are all above 0.6, which indicates an acceptable level in social sciences. The Second issue is the relationships between variables. Results indicated low values of beta between security/privacy and Trust. To make sure that the significance values are acceptable, a bootstrapping estimate is done, which is shown in Fig. 4.

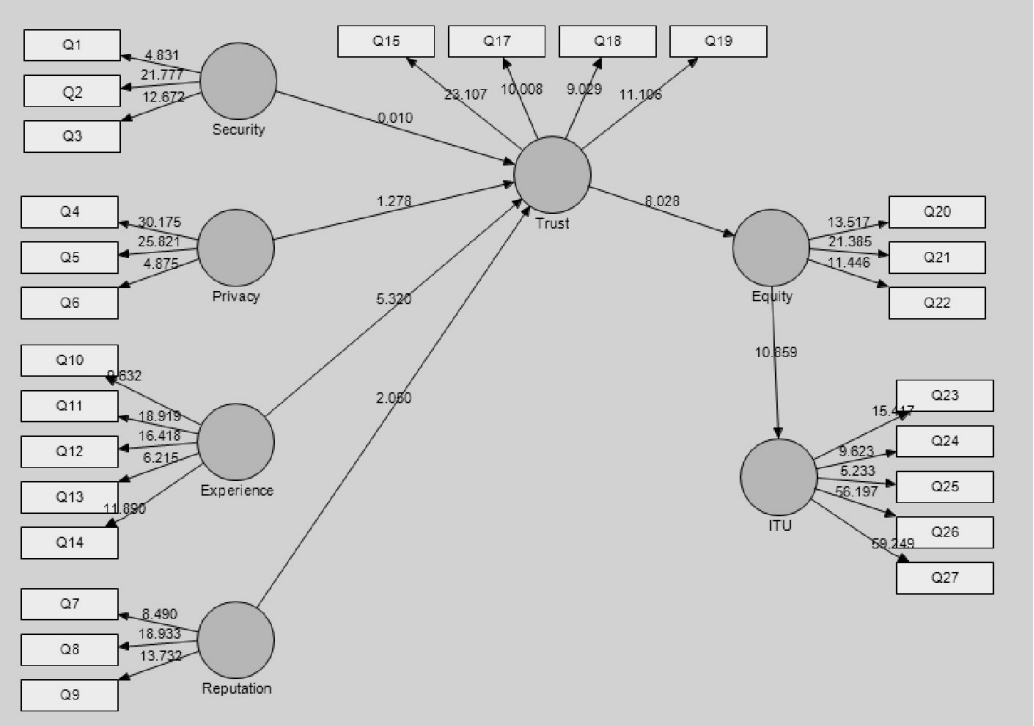

Fig. 4: The "t" values for all relaiosnhips
The model is estimated using SmartPLS (Ringle et al., 2005)

Results indicated that all loadings are significant at the 0.05 level (beta value above 1.96). Also, when we look at the loading on arrows between variables we can see that security and privacy are not significant predictors of trust. Only prior experience (beta = 0.569) and brand reputation (beta = 0.207) are significant predictors of trust and they explained trust with an R^2= 0.649. Such high value is a contribution of two new predictors of trust.

On the other hand, trust significantly predicted brand equity with an R^2 = 0.547, which equals the square of the beta value of 0.74. Also, on the same line, brand equity significantly predicted ITU cloud computing with an R^2 = 0.622 (again it is the square of 0.788). Our results indicates a full support of hypotheses H3-H6, but failed to support H1 & H2. The final research model resulting from this estimation is shown in Fig. 5.

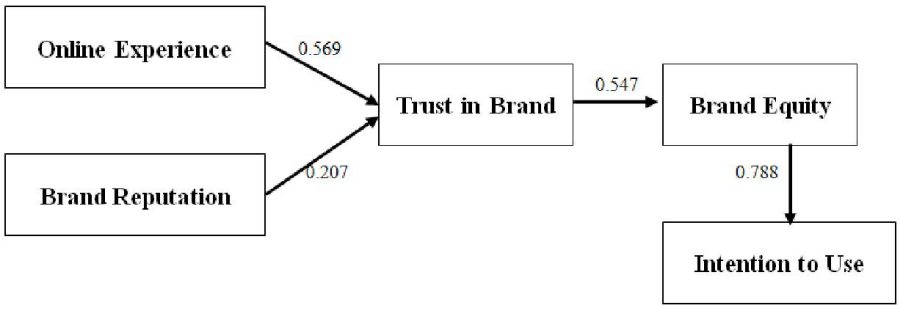

Fig. 4: The Final research model1 Fig. 4: The Final research model

Conclusions and Future Work

Cloud computing is emerging as a strategic choice for many organizations and for individuals, where many venders are offering Internet capacity to be used by users for free to save their data and information. It is still a concern for many to lose control over their data, where trust issues become vital. It is assumed that brand equity will be the ultimate definer of how people adopt certain cloud computing vender and if such factor (brand equity) will be influenced by the level of trust in the brand.

This paper tried to see if certain factors discussed in the literature are important in deciding on a brand and adopting it. Results of data analysis indicated that prior online experience and brand reputation are the major predictors of trust in a brand, while security and privacy failed to do so (total $R^2 = 0.649$). Also, trust in the brand significantly predicted brand equity (beta = 0.74, $R^2 = 0.547$) and brand equity significantly predicted intention to use cloud computing (beta = 0.788, $R^2 = 0.622$).

This study proposed 6 hypotheses and failed to support two of them. The inability to support H1and H2 can be attributed to the age of the sample used. 82.5% of our sample is younger than 40, and it has been shown repeatedly in literature that younger people have lower privacy and security concerns [24] [35]. Such issue calls for more research with larger sample and a test on age and other moderating factors.

This study suffered from the limitation of small sample, where users of cloud computing are still small compared to other IT applications. Also, the survey used is a new one and stated in Arabic language, where some respondents indicated that an English survey will do better when dealing with new technology. Based on that, future work should be emphasized to test the resulting model and see how security and privacy were not supported. Also, validating the new proposed instrument is essential when dealing with perceptional measures and subjective responses. Finally, brand equity showed a large explanation of variance in predicting the intentions to use cloud

computing, where more research is needed to see if other factors can influence such decision.

References

[1] Aaker, D. A., & Joachimsthaler, E. (2000). The Brand Relationship Spectrum: The Key To The Brand Architecture Challenge. *California Management Review*, 42 (4), 2-23.

[2] Abu-Shanab, E. & Pearson, J. (2007). Internet Banking in Jordan: The Unified Theory of Acceptance and Use of Technology (UTAUT) Perspective. *Journal of Systems and Information Technology*, Vol. 9 (1), 2007, pp. 78-97.

[3] Abu-Shanab, E. & Al-Azzam, A. (2012). Trust Dimensions and the adoption of E-government in Jordan. *International Journal of Information Communication Technologies and Human Development*, Vol. 4(1), 2012, January-March, pp.39-51.

[4] Abu-Shanab, E. & Ghaleb, O. (2012). Adoption of Mobile Commerce Technology: An Involvement of Trust and Risk Concerns. *International Journal of Technology Diffusion*, Vol. 3(2), April-June, 2012, pp. 36-49.

[5] Ailawadi, K. L., & Keller, K. L. (2004). Understanding retail branding: conceptual insights and research priorities. *Journal of Retailing*, 80 (4), 331-342.

[6] Alam, S. S., & Yasin, N. M. (2010). What factors influence online brand trust: evidence from online tickets buyers in Malaysia. *Journal of Theoretical and Applied Electronic Commerce Research*, 5 (3), 78-89.

[7] Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *Journal of Marketing*, 69, 133-152.

[8] Berry, L. L. (2000). Cultivating service brand equity. *Journal of the Academy of Marketing Science*, 28, 128-137.

[9] Christodoulides, G., Chernatonya, L. d., Furrerb, O., Shiua, E., & Abimbolac, T. (2006). Conceptualizing and Measuring the Equity Of The Online Brand. *Journal of Marketing Management*, 22, 799-825.

[10] Columbus, L. (2013, February 1). Roundup of Cloud Computing & Enterprise Software Market Estimates and Forecasts, 2013. Retrieved October 1, 2014, from Forbs: http://www.forbes.com/sites/louiscolumbus/2013/02/01/roundup-of-cloud-computing-enterprise-software-market-estimates-and-forecasts-2013/

[11] Cox, D. F., & Rich, S. U. (1964). Perceived Risk and Consumer Decision-Making—The Case of Telephone Shopping. *Journal Of Marketing Research*, Vol. 1(4), pp. 32-39.

[12] Craig, R., Frazier, J., Jacknis, N., Murphy, S., Purcell, C., & Spencer, P. (2009). "Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing". San Jose,CA, USA,: Cisco Internet Business Solutions Group (IBSG), Accessed from the Internet in 2014:http://www.cisco.com/web/about/ac79/docs/sp/Cloud_Computing.pdf.

[13] Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research* 59 (2006), pp. 877-886.

[14] Fitó, O., & Guitart, J. (2013). Business-driven Management of Infrastructure-level Risks in Cloud Providers. *Future Generation Computer Systems*, Vol. 32, 2013, pp. 41-53.

[15] Frăţilă, L. A., Zota, R. D., & Constantinescu, R. (2013). An Analysis of the Romanian Internet Banking Market from the Perspective of Cloud Computing Services. Procedia Economics and Finance, 6, 770-775.

[16] Gummerus, J., Liljander, V., Pura, M., & Van Riel, A. (2004). Customer loyalty to content-based web sites: the case of an online health-care service. Journal of services Marketing, 18(3), 175-186.

[17] Ha, H. Y. (2004). Factors influencing consumer perceptions of brand trust online. Journal of Product & Brand Management, 13(5), 329-342.

[18] Heiser, J., & Nicolett, M. (2008). Assessing the Security Risks of Cloud Computing. Retrieved December 10, 2013, from Gartner group: https://www.gartner.com/doc/685308

[19] Iliff, R. (2014). 4 Reasons Online Brand Equity Matters. Retrieved October 10, 2014, from: University of Ilinois at Urbana-Champaign Office of Technology Management: http://otm.illinois.edu/blog/otm-guest-blog-4-reasons-online-brand-equity-matte.

[20] Jevons, C., & Gabbott, M. (2000). Trust, brand equity and brand reality in internet business relationships: an interdisciplinary approach. Journal of Marketing Management, 16(6), 619-634.

[21] Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 1(2), 53-58..

[22] Kumar, S., & Goudar, R. H. (2012). Cloud Computing–Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication, 1(4).

[23] Kuyoro, O., Ibikunle, F., & Awodel, O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks (IJCN)*, Vol. 3(5), 247-255.

[24] Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage. Qualitative Market Research: An International Journal,5(4), 291-300.

[25] Madhavaiah, C., Bashir, I., & Shafi, S. (2012). Defining Cloud Computing in Business. *The Journal of Business Perspective*, 16(3), pp. 163-173.

[26] Madhavi, K. V., Tamilkodi, R., & Jaya Sudha, K. (2012). Cloud Computing: Security threats and Counter Measures. IJRCCT, 1(4), 125-128.

[27] McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security

concerns. Journal of Business Research, 63(9), 1018-1024.

[28] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. Retrieved December 5, 2013, from the website Computer Security Division. U.S. Department of Commerce) Retrieved December 5, 2013, from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[29] Mishra, B., & Mishra, V. (2012). Implement Cloud Computing Model For Business Information System Security. *International Journal of Current Research*, Vol. 4(11), pp. 121-125.

[30] Mahmud Mohammadian, M. G. (2014). A Study of Factors Influencing Online Brand Trust in Online Service Retailing. NATIONALPARK-FORSCHUNG IN DER SCHWEIZ (Switzerland Research Park Journal), 103(2).

[31] Morgan-Thomas, A., & Veloutsou, C. (2013). Beyond technology acceptance: Brand relationships and online brand experience. Journal of Business Research,66(1), 21-27.

[32] Park, J., & Stoel, L. (2005). Effect of brand familiarity, experience and information on online apparel purchase. International Journal of Retail & Distribution Management, 33(2), 148-160.

[33] Parsi, K., & Laharika, M. (2013). A Comparative Study of Different Deployment Models in a Cloud. International Journal of Advanced Research in Computer Science and Software Engineering, 5(3), 512-515.

[34] Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. Management Information Systems Quarterly, 31(1), 105-136.

[35] Pingitore, G., Meyers, J., Clancy, M., & Cavallaro, K. (2013) Consumer Concerns About Data Privacy Rising: What Can Business Do?. Retrieved October 29, 2014, from *McGraw Hill Financial Global Institute*: http://www.mhfigi.com/wp-content/uploads/2013/10/MHFIGI-Data-Privacy-Concerns-FINAL.pdf.

[36] Posey, M., & Chen, G. (2012) Parallels Private Vendor Watchlist Profile: Helping Service Providers Compete in the Cloud. Retrieved October 29, 2014, from IDC Analyze the Future: http://sp.parallels.com/fileadmin/parallels/documents/idc/IDC_Parallels_Private_Vendor_Watchlist_Profile_-_Helping_Service_Providers_Compete_in_the_Cloud_-_document_233149_-_Feb._2012.pdf.

[37] Qaisar, S., & Khawaja. (2012). Cloud Computing: Network/Security Threats and Counter Measures. Interdisciplinary Journal of Contemporary Research in Business, 9(3), 1323-1329.

[38] Qasim, H., & Abu-Shanab, E. (2014). Cloud Computing Risks & Business Adoption. International Journal of Emerging Sciences, 4(2), 52-63.

[39] Rabai, L., Jouini, M., Aissa, A., & Mili, A. ". (2013). Cyber-security model in cloud computing environments. Computer and Information Sciences, 25(2013), 63-75.

[40] Riahi-belkaoui, A., & Pavlik, A. (1991). Asset Management Performance and Reputation Building for Large US Firms. British Journal of Management, 2(1991), 231-238.

[41] Ringle, Christian Mark/Wende, Sven/Will, Alexander (2005). SmartPLS, release 2.0 (beta), accessed from the Internet http://www.smartpls.de, published by SmartPLS, Hamburg, Germany.

[42] Rios, R., & Riquelme, H. E. (2010). Sources of brand equity for online companies. Journal of Research in Interactive Marketing, 4(3), 214-240.

[43] Rubel, S. (2014, 8 1). In the Era of Cloud Computing, Three Important Maxims for Brands to Follow. Accessed from the Internet in 2014 from: http://adage.com/article/digital/cloud-computing-security-important-brands/228406/

[44] Ruparelia, N., White, L., & Hughes, K. (2012). Drivers of brand trust in Internet retailing. Journal of Product & Brand Management, 19(4), 250-260.

[45] Ruyter, K. d., Wetzels, M., & Kleijnen, M. (2001). Customer adoption of e-service: an experimental study. International Journal of Service, Industry Management, 12(2), 184-207.

[46] Sharma, M., Bansal, H., & Sharma, A. K. (2012). Cloud Computing: Different Approach & Security Challenge. International Journal of Soft Computing and Engineering (IJSCE), 2(1), 421-442.

[47] Sharon, Y. (2012). Move into the Cloud, shall we? Library Hi Tech News, 29(1), 4-7.

[48] Sinjilawi, Y., AL-Nabhan, M. & Abu-Shanab, E. "Addressing Security and Privacy Issues in Cloud Computing". Journal of Emerging Technologies in Web Intelligence, 6(2), May 2014, 192-199

[49] Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law& Security Review, 26(2010), 391-397.

[50] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(2012), 583-592.

Appendix A

Privacy & Security:	References used
I intend to checked check the security item before I sign up on a drive	Ruparelia, White, & Hughes (2012) Alam & Yasin (2010) Bart, Shankar, Sultan, & Urban (2005)
I feel secure when I provide personal information on a drive	
The CC site I use is protected against hacking	
I feel that my privacy is protected when I use a drive	
I am confident that my personal information will not be shared with other organizations when I use a drive	
I intend to read the privacy policy Before I signed up for a drive The drive privacy policy is easy to read and understand	
Brand reputation	References used
I think the drive I use has a good reputation	(Alam & Yasin, 2010) (Morgan-Thomas & Veloutsou, 2013)
The think that it one of the leading cloud vendors	
I think that the drive I use offers high quality services	
Users' experience	References used
My previous use of Google drive was satisfying	Alam & Yasin (2010) Christodoulides, Chernatonya, Furrerb, Shiua, & Abimbolac (2006) Morgan-Thomas & Veloutsou (2013)
My previous use of Google drive was exiting	
The layout of the drive page is appealing	
The Google drive page can be personalized	
I find that Google drive is easy to use	
Brand trust	References used
I trust the drive I use and its services	Ha (2004) Alam & Yasin (2010) Ruparelia, White, & Hughes (2012)
I feel comfortable using their services	
I prefer that using this drive than using any other cloud vendor	
The drive I use keeps its promises	
My interest is a priority for the	

drive vender I use	
Brand equity	References used
I think that the drive I use is reliable	Ha (2004) Rios & Riquelme (2010)
I think that the drive I use is dependable	
I believe that the drive I use offers valuable services	
Intention to use	References used
On the basis of this description, I would continue using this drive	Abu-Shanab & Pearson (2007)
I would tell interested friends to use of this drive	
I will strongly recommend it to others	
I expect that I will use this drive in the future	
I plan to use this drive in the future	