Analysing security risk of a cloud computing system to produce a model for secured business environment

R. Senthilkumar[1],
Department of Information Technology,
Higher College of Technology (HCT),
Muscat, Sultanate of Oman
senthilkumar75.mca@gmail.com

S. G. Kiran Kumar[2],
Department of Information Technology,
Higher College of Technology (HCT),
Muscat, Sultanate of Oman
kiran43427@gmail.com

Dr. Binod Kumar[3]
Department of Information Technology,
Higher College of Technology (HCT),
Muscat, Sultanate of Oman
binodkr75@gmail.com

Abstract

These days, almost all the medium and big size of businesses is using the cloud computing system to run their business across the globe and around the clock. It becomes popular and of huge application due to its characteristics such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. This is an affordable and effective place for businesses to sell and promote their goods and services.

However the security problems for the cloud computing system are very significant. It can ruin the rapid development of cloud computing. In Business, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. The data privacy and service availability in cloud computing are the key security problem. The internet also provides opportunities for fraudulent behaviour and unauthorized access to business and client data. Attacks on the computer system of a business can have immediate and ongoing effects, such as targeting customers for identity crimes or infecting website visitors with malicious software. Due to having combination of various types of models in the cloud computing, the single security method cannot solve its security problem. Various traditional and new technologies and strategies together need to consider for protecting a cloud computing system totally.

The aim of this paper is to bring into the deep sight of the cloud computing systems working and then to analyse the cloud computing security problem and its strategy according to the cloud computing concepts and characters. In addition to that, we are identifying the higher vulnerabilities in this type of systems and the most important threats found in the literature study related to Cloud

Computing and its environment as well as to identify and relate vulnerabilities and threats with the possible solutions.

Keywords: Cloud computing, Security, Key Problems, Vulnerabilities, Threats, Counter measures.

1. Introduction

These days, almost all the medium and big size of business are using cloud computing system to run their business, across the globe and around the clock. It is an affordable and effective place for businesses to sell and promote their goods and services. It gives pleasure of easy to manage the stocks for the trader and an essay method of selecting, ordering the item and paying its bill for the customer. Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. It becomes popular and of huge application due to its characteristics such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. Cloud computing offers a number of benefits to businesses. For example, data and applications can be accessed anywhere and there are cost benefits in not having to purchase, maintain, install and update hardware infrastructure or software applications. It is predicted that the uptake of cloud computing will increase, with asserting that cloud computing also offers significant computing capability and economy of scale that might not otherwise be affordable to business, especially for small and medium enterprises that may not have the financial and human resources to invest in IT infrastructure.

However this system has significant security problems that an enterprise need to measure otherwise it can ruin the rapid development of cloud computing. Cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. The data privacy and service availability in cloud computing are the key security problem. So there is a need to design a secure and safe business environment where both the customer and trader should do the trading without losing their assets as well as the privacy. There is a robust, reliable and protective business environment need to develop. To design this system we can select out of the hardware, software and network tools that is best suiting for our requirement. To enhance its scale of working that can protect a business completely, we can integrate and/or deploy these into the business system, and if required we can also grid these with hi speed network.

In this paper first, we are discussing the architecture of a Cloud computing system and its related tools, techniques and mechanisms that is used to develop a cloud computing system. Latter, we are analysing and assessing all these in terms of providing a secured business environment both for trader and the customer. Finally, we are identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.

2. Architecture

Cloud computing refers to the access to network storage and applications online. The cloud computing is an integrated computing model that is produced by integrating grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies. It has large scale computation and data storage, virtualization, high expansibility. Services on Cloud system are stored on servers in large data warehouses and are accessed via the internet, with users paying providers only for what they use. There are three primary types of cloud offerings, First, Software as a Service (SaaS), Second, Infrastructure as a Service (IaaS) and third, Platform as a Service (PaaS). Major components of a cloud computing system are Pay as you go; Access from anywhere anytime any device; Economy of scale, Flexibility and Expertly Managed.

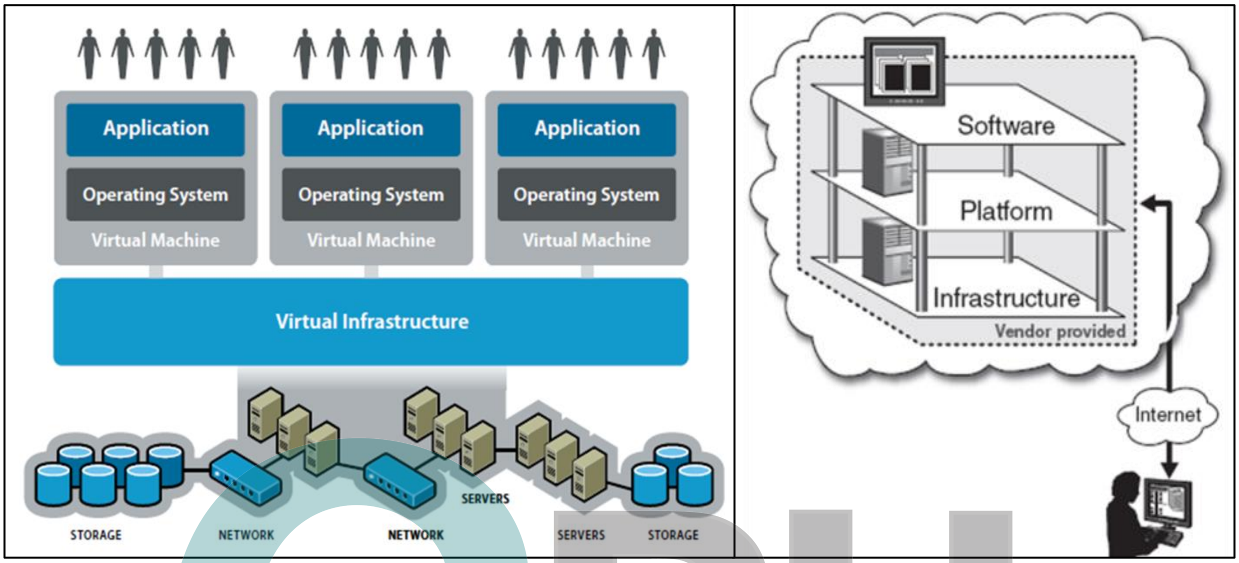


Figure 1: CLOUD COMPUTING ARCHITECTURE

Working of Infrastructure-as-a-Service (IaaS):- A service model that involves outsourcing the basic infrastructure used to support operations--including storage, hardware, servers, and networking components. The service provider owns the infrastructure equipment and is responsible for housing, running, and maintaining it. The customer typically pays on a per-use basis.

Working of Platform-as-a-Service (PaaS):- A service model that involves outsourcing the basic infrastructure and platform (Windows, Unix). PaaS facilitates deploying applications without the cost and complexity of buying and managing the underlying hardware and software where the applications are hosted.

Working of Software-as-a-Service (SaaS):- Also referred to as “software on demand,” this service model involves outsourcing the infrastructure, platform, and software/applications. Typically, these services are available to the customer for a fee, pay-as-you-go, or a no charge model. The customer accesses the applications over the internet.

3. Cloud Computing Risks (Challenges)

In this system, Internet is an affordable and effective place for businesses to sell and promote their goods and services. However, the internet also provides opportunities for fraudulent behaviour and unauthorized access to business and client data. Attacks on the computer system of a business can have immediate and ongoing effects, such as targeting customers for identity crimes or infecting website visitors with malicious software. Cloud computing refers to the access to network storage and applications online. There are various kind of risks associated with the use of cloud computing. For example providers may be vulnerable to malware infection and attacks that result in unauthorized access to the data held in their servers; if internet connectivity is lost, businesses would be unable to access their data or applications; businesses lose control over the security of their data; data may be misused by rogue providers; data may be insecurely transmitted, stored or processed by the provider; and legal jurisdictional issues may arise when the provider is foreign owned or the data are stored or transmitted overseas.

Database Security threats: - A few warehouses contain customer-ID/user passwords with very unsafe manner. When some intruder or hacker gets user authentication information, then he/she can misuse the secured data imposing as the authorized client/user and reveal private and information. E-business machines contain clients' information and get valuable data through information pools that are linked to the Internet server. Rather business data, information pools linked to the Internet has important and safe data which can spontaneously destroy a corporate as they are destroyed, obtained and changed.

Online fraud: - There are a number of scams that businesses may be vulnerable to and many of these are being committed over the internet or by email. Some of the online scams targeting businesses are card-not present fraud, overpayment and upfront fee scams. Compromised credit card details may be used online for fraudulent card-not-present transactions, where account information is used without the authority of the cardholder. Overpayment scams involve ordering goods and the scammer paying more than the agreed amount using a counterfeit or dishonourable cheque, or money order or stolen credit card. The seller is then out of pocket if they post the goods and refund the overpaid amount before the payment is cleared.

Threats: - Businesses may lack the expertise to identify and deal with computer security incidents making them an attractive target for online offenders. An overview of some of the threats faced by small businesses, including the nature of the threat and potential outcomes, is provided in the following section. Scenarios include malware infection, wireless internet misuse and session hijacking, online fraud, compromised websites, denial of service attacks, phishing, spear phishing, unauthorized access and risks associated with cloud computing. While this overview is not exhaustive, it aims to increase awareness of the types of vulnerabilities small business operators may face.

Instant Messaging (IM):-Communication tool Products like WhatsApp, Facebook, and Messenger etc. provide a convenient way to communicate with others in real time. These emphasizes functionality over security and placing enterprise systems at risk to hackers, viruses, worms, Trojans, legal liability and violation of privacy laws.

Phishing and Electronic Identity Theft:- Mass e-mailing sent by phishers, looks as sent from banks, mortgage companies, brokerage firms, ISPs, or other legitimate organizations with which the recipients may do business, such as Citibank, PayPal, etc. It get divulge information like account id and passwords.

Malware: - Malicious software, perform unwanted actions and installed without the user's permission. It includes programs like Trojan horse, spyware and adware. It changes settings of a computer connection so that it will access its data and information.

Viruses and Worms: - Small unwanted programs. Replicate themselves and spread through e-mail, HTML mail, online P2P file sharing, instant messages, Windows file sharing, or files downloaded from Web sites, FTP sites, newsgroups, or other sources. It may lie dormant until a particular date or time or specific circumstances trigger them. It damage files, crashing programs, or flooding networks with so much traffic.

Trojan Horses: - One kind of malware often installed along with free software. It creates a back door for hackers; send sensitive information to the hacker.

Adware and Spyware: - Software products display advertising, installed along with another downloaded or bought program. It changes browser's home page; collects and transmits system information.

Cookies: - Small text files placed on computer by web sites to retain site-entered information. Ii tracks web activities and target advertising to us based on our activities.

Denial of Service Attacks: - It involves flooding a system or network with more data than it can handle. Example Buffer overflow, SYN flood, Teardrop attack and Smurf attack. System crashes or network bandwidth is so clogged.

Spoofing: - A mechanism, used by attackers to disguise the origin of an attack. Examples are IP spoofing, E-mail spoofing, and Web spoofing. IP spoofing involves forging the source IP address on data sent over the network so that it appears to come from a different computer or network. E-mail spoofing involves changing the header information on e-mail messages to make them appear to come from someone other than the true sender. Web spoofing involves attackers creating false copies of a Web site or entire Web which they control, so that victims are actually visiting the attacker's Web server when they think they are visiting a legitimate Web site on a different server. It enables to disguise the origin of an attack.

Port Scanning:-A port is a logical point of connection that is used by network applications for communications between two computers. It enables attackers to enter the system through an open port.

Password Cracking:-A method based on commonly used passwords or personal information about the user, such as the name of a spouse, child, or pet, or a social security or phone number. Other methods are dictionary attacks, brute force attacks and social engineering. It enables outsiders to work as an authorized user/administrator.

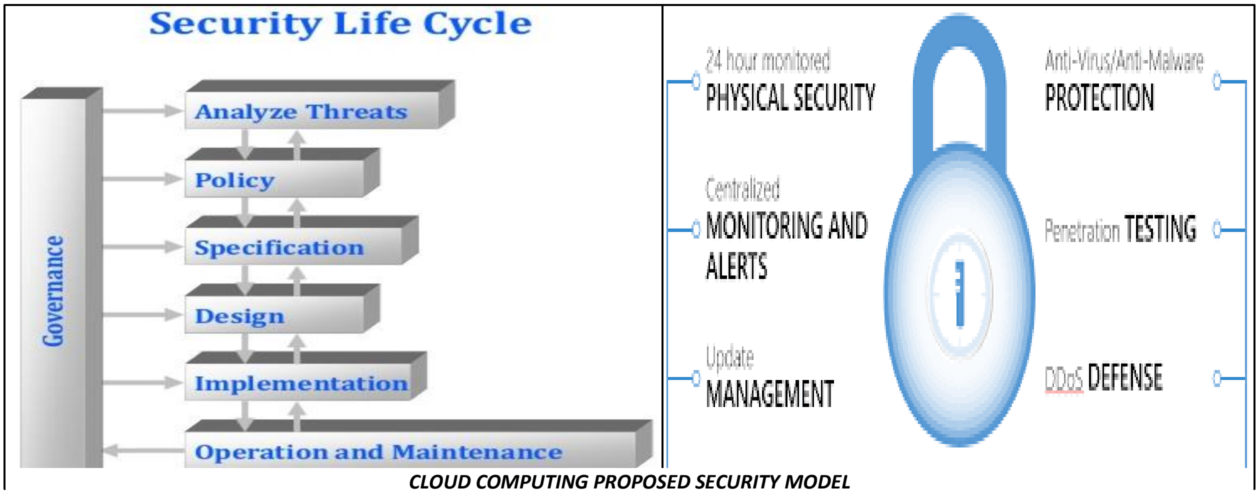
Hack Attacks: - Specific attacks used to gain access or bring down a computer system or network. It intercepts messages and then modifies it. Crash a system or take control of it.

Social Engineering: - It is an art of persuading people to divulge information, such as account names and passwords. It allow the hackers to access a system or network

4. Proposed System Design

There is a robust, reliable and protective business environment system need to develop. To design a reliable secured and threats free business model we can select out of the hardware, software and network tools that is best suiting for our requirement. Business need to put computer security on high priority else the outcomes of a security incident, such as websites not being accessible and loss of reputation can have a significant impact on a business. This is particularly the case for businesses conducting the majority of their trade or advertising online. It is also important to recognize that the harm caused by computer security incidents can extend beyond damage to business. For example, there is also the increased proliferation of malware, botnets and identity crimes when websites and computer systems are compromised. The cost of a multifaceted security strategy that is regularly reviewed and updated may be trivial compared with the financial and intangible losses following a computer security incident and may not necessarily be that difficult to enact.

To enhance its scale of working that can protect a business completely, we can integrate and/or deploy these stated in above pictures into the business system, if required we can also grid these with hi speed network. Also, a policy and paradigms and training for the business staffs need to prepare. A cost-effective strategy could consist of the implementation and regular review of following:-



CLOUD COMPUTING PROPOSED SECURITY MODEL

Technical prevention measures:—ensuring application and operating system patches are up-to-date and automated, enabling firewalls, using effective anti-malware software, providing secure sites so that customers can provide their personal information safely and restricting administrative privileges for IT systems.
Organizational policies and staff training: — informing employees about the proper and secure use of business resources, password management and user access.

Physical security:—restricting access to IT hardware and infrastructure.

Apart from these as demonstrated in this paper, businesses still have some way to go to ensure that they remain safe in the ever-changing online environment. The risks for businesses and their online customers

5. Conclusion

Cloud Computing provides computing as a service while allowing proven experts to manage data-centres efficiently. In Business it is an affordable and effective place to sell and promote their goods and services. It has number of benefits to businesses example like data and applications can be accessed anywhere and there are cost benefits in not having to purchase, maintain, install and update hardware infrastructure or software applications.

However it has huge security problems that need to assess and countermeasures need to apply to overcome that else it can harm both trader and customer, and can ruin the rapid development of cloud computing. By assessing the existing security problems and threats and finding counter measures for these, a reliable, robust and secured business environment can be develop where hassle free trading.

6. References

[1]. ACM Tech Pack on Cloud Computing Ajay Mohindra, IBM Research Division, Thomas J. Watson Research Center Chair, ACM Tech Pack Committee on Cloud Computing Copyright © ACM 2015

[2]. A REVIEW OF CLOUD COMPUTING SECURITY ISSUES, Manpreet Kaur etl, International Journal of Advances in Engineering & Technology, June, 2015On Security Issues in Web Applications through Cross Site Scripting (XSS), IEEE, Published in: Software Engineering Conference (APSEC), 2013 20th Asia-Pacific (Volume:1)

[3]. An analysis of security issues for cloud computing, David G Rosado, Eduardo Fernández-Medina et al, Journal of Internet Services and Applications,http://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5, 27 February 2013

[4]. Cloud Computing and Security, Venkat Reddy Melachervu et al, ISACA Hyderabad, Jul 21, 2013

[5]. Data Security and Privacy in Cloud Computing, Yunchuan Sun et al, International Journal of Distributed Sensor Networks Volume 2014 (2014), Article ID 190903, 9 pages, http://dx.doi.org/10.1155/2014/190903, 2014

[6]. Microsoft cloud services and network security, azure.microsoft.com

[7]. Research on cloud computing security problem and strategy, W. Liu ; Dept. of Comput.. & Inf. Eng., Wuhan Polytech. Univ., Wuhan, China, 21-23 April 2012

[8]. Special issue on security in cloud computing, Jaatun et al. Journal(Springer) of Cloud Computing: Advances, Systems and Applications 2012

[9]. Security Issue for cloud computing , Kevin Hamlen, Murut kantarcioglu, The University of Texas at Dallas, Feb 2010

[10]. Study and Analysis of Various Security models for better Alignment and Effectiveness, Dr. Binod Kumar, Kanak Saxena, PhD Thesis Report, Barakkat Ullah University, M.P. India, Jan 2009

[11]. Security Issues of IEEE 802.16 (WiMAX),Jamshed Hasan, Edith Cowan University, Australian Information Security Management Conference, 2006.

[12]. Trends & issues in crime and criminal justice, Australian Government, Australian Institute of Criminology, No. 433 February 2012