Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-69

Trust relationship model to enhance security and privacy for cloud environment

Dana Al-Tehmazi ,Huda Al-Jobori

***Abstract*—These days the common term used for distinguishing the services such as availability, data mobility, cost effective, privacy and security is "Cloud Computing Technology". Cloud computing can solve technical issues, reduce organization cost, and make data available anytime, anywhere. Like many technologies, cloud computing is facing lot of challenges; one of these challenges is "Trust relationship". In this paper we will propose a model called "Cloud Computing Trust Relationship Model (CCTRM)". This model will enhance the security and privacy for cloud computing environment. CCTRM model will be used in telecommunication and non-telecommunication organizations, governments sectors, and private sectors to implement trust relationship between them and cloud computing service providers. This trust will allow the organization to obtain cloud computing services safely without the need to be worry about security and privacy on their cloud.**

Keywords: **Cloud Computing, Trust Relationship, Trust Model, Infrastructures as a Service.**

I. Introduction

Information Technology (IT) has been in place since the usage of first mainframes computers in 1960s. Then developed to minicomputers, personal computers (PC), client servers, Internet Protocol (IP) Networks, mobile devices, grid computing and now we are in Cloud Computing era. Cloud computing provides all the resources such as hardware platform, infrastructure, application and software required for business computing wherever and whenever they are needed. The evolution of cloud computing has already started and can completely change the way organizations are using the technology to cloud service provider (CSP) and customer.

Cloud computing have many services, to offers, such as Software as a Service (SAAS), Infrastructures as a Service (IAAS), Platforms as a Service (PAAS), Security as a Service, Storage as a Service, IT as a Service, Desktop as a Service, and other services. In each service in the cloud, there are terms and conditions between the CSP and customer.

Security, privacy and trust are very important elements in cloud computing, especially when it comes to customer data.

Dana Al-Tehmazi
Society of Information Technology,
IEEE Bahrain Section, Manama, Kingdom of Bahrain

Huda Al-Jobori
Department of Information Technology,
Ahlia University, Manama, Kingdom of Bahrain

Most ministries, educational institutions, financial and banking organizations in any countries are concerning about keeping their own data in the cloud due to reasons such as, security of cloud datacenter, location of cloud, trusting CSP, and various other reasons. In this paper our main focus is about implementing trust relationship through a model to enhance security and privacy for cloud computing environment. Moreover, our prototype which we will use in this paper to implement our model is a local *organization* in Kingdom of Bahrain.

This paper is organized as follows: Section (II) will discuss the related research papers which are supporting the trust relationship in cloud computing. Section (III) will define and introduce trust elements. Overview of proposed trust relationship model is presented in section (IV). Section (V) will discuss a case study for organization proposed to implement CCTRM model in their organization infrastructure. Finally conclusions and future work are show in section (VI).

II. Literature Review

In recent years, many research papers and thesis have made a lot of study on trust model computing the trustworthiness of trusting cloud services and managing the trust relationship. Santos et al [1], they proposed a design to trust the cloud and they called it: Trusted Cloud Computing Platform (TCCP) to ensure the confidentiality and integrity. One feature of this design is to allow IAAS providers to provide a closed box execution environment that will guarantee confidential execution of guest virtual machines. Besides, it allows users to verify the IAAS provider and decide whether or not the service is secure before they launch their virtual machines.

Yang et al [2], introduced three layers for trust conceptive framework in which it includes both the validity of the "hard trust" to guaranteed security mechanisms and technical devices, and "soft trust" that ensure by social legal human factors, Plus considering "trust relationship" between customers and cloud vendors, through the combination and integration of the three trusted layer in framework model. They also reported that the gap between these trust factors can be bridged from the underlying infrastructure to the virtual systems and to the service interaction level, to the trust field in cloud environment.

Siani paper [3], evaluated the security, trust and privacy issues that happen in cloud computing; in addition, proposing some approaches to address them. These approaches demand that there should be consistent and coordinated development between: Innovative regulatory frameworks such as

SEEK DIGITAL LIBRARY

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-69

accountability between operation of global business and provision of reform within cloud environments. Responsible company governance whereby organizations act as responsible host of the data which is entrusted to them within the cloud environment, by ensuring responsible behavior via accountability mechanisms, and balancing innovation with individuals expectations, privacy and being a way of achieving trust. Lastly, Supporting technologies by including privacy enhancing security mechanisms, technologies, encryption, and anonymization.

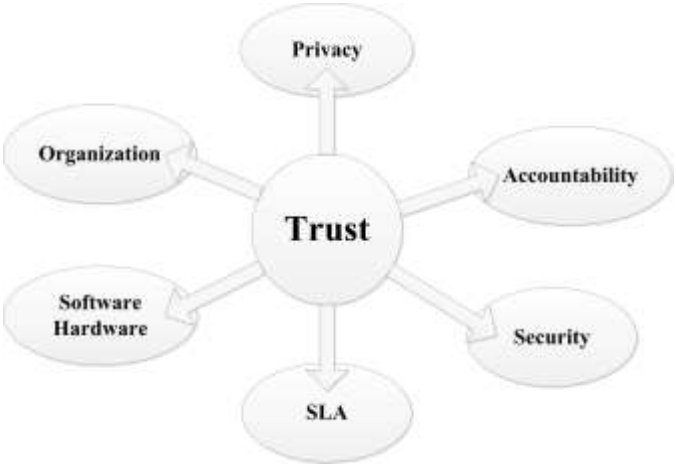
Pearson et al [4], discussed the key challenges in achieving trusted cloud through the use of detective controls, to identify the appearance of a privacy and security risk that goes against the privacy or security policies and procedures. Beside clarifying the three main components which affect the cloud trust (Security, Privacy, and Accountability). Then focusing in their proposed model which is "Trust Cloud Framework for accountability", and this framework consists of four accountability abstraction layers, initialing with System Layer, Data Layer, Workflow Layer, and ending with policies Law and Replications Layers. This model can be used to give cloud users a single point of view for accountability of the cloud service providers.

Li and Ping [5], analyzed in their paper several trust models used in big and distributed cloud environments and they introduced a new cloud trust model to solve security issues in cross clouds environment in which cloud customer can choose different resources and service providers in various domains. Their model is domain-based where it divides one cloud service providers nodes into the same domain and set trust agent. It distinguishes two different cloud customer roles and cloud servers, beside designing different strategies for both of them. Moreover, the proposed model is treated as one type of cloud service provider just like storage or computation. The model achieves both behavior authentication and identity authentication. Finally, their results show's that the proposed model can safely and efficiently construct trust relationship in cross clouds environment.

Sun et al [6], introduced trust management model based on a set of theories that included direct trust measurement, computing connecting, and trust chain integrating. This model aims toward the cloud users who are making their own decision on whether to use cloud services from some cloud service provider by giving them trust evaluation groups about cloud providers and then build sensible trust relationship between them. This proposed model is a new idea of how to implement trust management in cloud computing environment.

III. Trust Relationship Elements

The elements used for proposed trust relationship model are six elements, (Privacy, Accountability, Security, SLA, Software/Hardware, and Organization). The model elements are displayed in figure (1).



Figuer 1. CCTRM elements

1) *Privacy:*

Privacy is to keep your information data in safe place where no one can reach them and protect them from unauthorized people.

As Tim Mather[7] says "You can have security and not have privacy, but you cannot have privacy without security". Ben Halpert [8] "The personal life of every individual is based on secrecy, and perhaps it is partly for that reason that the civilized man is so nervously anxious that personal privacy should be respected". As a result, Privacy refers to the right of self-determination, that is the right of individuals to 'know what is/are known about them', be aware of their stored data, control how that data and information are communicated and prevent from any attack. In additional, it refers to more than just privacy and confidentiality of information data. Protection of personal data derives from the right to privacy via the associated right to self-determination. Every individual user has the right to control their own data, whether its public, private, or professional data.

The data is a set of variables, quantitative, qualitative and values. Data can be explained in many ways, such as data in computing world, data in personal life, data in mathematics reports, data in business, Internet data (broadband data), and many other data's which the individuals are using in their daily life. These data are the formation of database stored in physical or virtual servers in the cloud. For example, when the individuals are using their mobiles to access their emails they essentially makes many processes either sending emails, saving contacts, deleting emails, adding pictures, adding numbers, etc. After entering these data it becomes as set of information in the cloud storage when it synchronized with their cloud ID such as Gmail id or LinkedIn id.

Furthermore, privacy is divided into two parts: Data privacy and Information security privacy. These two main aspects will affect privacy in all the conditions as they were shown in many researches and experiments. The data privacy and information security privacy are connected together for official and

SEEK DIGITAL LIBRARY

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-69

personal use, to collect, disclose, save, delete and storing information data [7].

In other words, privacy is about accountability and transparency to individuals or organizations especially when it comes to cloud environment, privacy is always the substance to a lot of consideration from cloud provider. Figure (2) shows Privacy Structures.

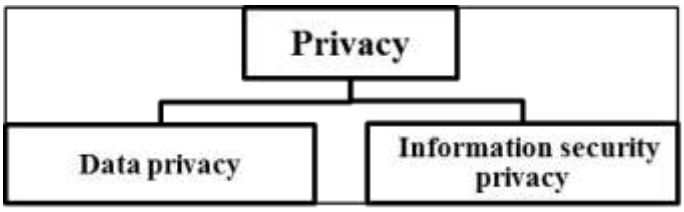


Figure 2. Privacy Structure

2) *Accountability:*

The other word of Accountability is Responsibility. It means that every organization or individual is accountable and responsible for their own self and especially for their data. The definition of accountability is "*the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information."*[9].

For example, the security policy for local organization states that all employees must avoid installing games and chat application on a company infrastructure device such as laptop, tablet, servers, etc. The responsibility of the system administrator in the organization is to keep an eye on the behavior of employees while they are using the internet, network and also checking the security policy if it's being followed as instructed .

To gain accountability to access any resource either this resource is stored in the cloud or not, two steps must be achieved: ***verifying identification*** of user either by user-name or account number. Providing two or more credential set to ***authenticate*** user with the system such as password, cryptographic key, or personal identification number (PIN). If the system determines that the user can access the resource, then the user is ***authorized*** and eligible to access the resource because the system checks the rights and the privilege for the user. So in this case the user will be accountable [10].

The technical mechanisms for accountability in cloud computing can include encryption and decryption methods for data security and privacy. Moreover, accountability can provide transparency between CSP and customers if they trust each other and CSP achieve their obligations towards their customers. E.g. Cloud Platforms Social Networks (CPSN) are scalable cloud applications hosted by profitable clouds such as Facebook (FB). The applications of (FB) are hosted by Amazon Web Service (AWS) platform, and the design architecture for Facebook application in social cloud computing network is typically similar to (PAAS) architecture [11]. Application programming Interface (API) of (FB) provides a set of information about users such as the friends list, groups, application users, events, photos, and profile information [12]. The (FB) programming language is a subset of Hypertext Markup Language (HTML) Markup language with Facebook Java Script (FBJS). Such infrastructure and platform cannot be used in an environment where customers need some level of accountability for the reason that there are no Service Level Agreement (SLA) between customer and (FB) provider, it's only about using free application in the cloud and customer can control their security setting for their account [13].

3) *Security:*

Security is an important element for establishing trust in any organization, between individuals and CSP, for the reason that, if security policy in CSP is strong then the trust will be strong too, and the customer will deal and trust CSP without concern about their data in the cloud. Security is about a model called Confidentiality, Integrity, and Availability (CIA) model. This model designed to guide and control policies for information security within an organization [10]. Therefore, confidentiality is a set of rules that restrict access to information; Integrity is the guarantee that the information is accurate and trustworthy. Availability is an assurance of ready access to the information by authorized individuals.

3.1) ***Confidentiality:*** is to linked data that has confidentiality and privacy to assure that private information of individuals or organizations are not available to unauthorized users. This is to assure that individuals can control and monitor their own data. For instance, the *social engineering attack* is happening when a user tricks another user into *Sharing Confidential Information* (SCI), by pretending that someone authorized the user to have access to their secured information. This attack take one-to-one communication medium method that used to perform social engineering attacks [14].

3.2) ***Integrity:*** is connecting data integrity and system integrity to assure that information and programs are changed and specified in authorized way. Also to assure that the system integrity performs perfectly and deliberates from unauthorized manipulation of the system.

The system's integrity will be compromised. For example the users usually affect a system or data's integrity by mistake for any instance. If the user insert unfitting values into a data processing application that will end up charging a customer $3,000 instead of $300. Another example if an employer with a filled hard drive may inadvertently delete some configuration files by assumption mistake, such as deleting a boot.ini file because the user don't remember ever using it.

Security should be more simple to customers capabilities to give them only certain sets and functionality. As a result, the mistakes become less devastating and less common. The system and critical files must be kept in secure and restricted place from viewing and accessing by any unauthorized users. In

SEEK DIGITAL LIBRARY

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-69

other words, the applications should arrange a mechanisms that will check validity and input values [10].

3.3) ***Availability:*** is to ensure accurate maintenance to all hardware and software in an organization and to perform hardware repairs immediately when needed. To provide a certain measure of redundancy and preventing the occurrence of bottlenecks and also providing suitable communications bandwidth to implement emergency backup for data lost and emergency backup for power systems in organization [10]. Alongside to keep current power with all necessary system upgrades, and guarding against unauthorized person and malicious actions such as Denial-of-Service (DoS) attacks [14]. For example, In Japan 2011 Tohoku earthquake and tsunami resulted the biggest power plant incident and it has caused the highest economic loss in history from any earthquake (over $300 billion USD). Moreover, this earthquake caused the highest death toll from any developed country (HDI>0.8) by approximately 3 times. Such disasters affected the country economics and business especially for governments and big companies, if they didn't have a disaster recovery plan for their data and infrastructures [15].

Achieving security CIA model are important to implement trust in cloud computing between CSP and customer.

4) *Service Level Agreement (SLA):*

SLA can be define as a document characterizing the level of service predictable or expected by a customer from a provider, placing out the standards in which that service is measured, and the penalties or remedies if any failure to meet the expectations. Generally, SLAs are between two indivials or external suppliers and companies [16].

For example, the SLA of internet exchange companies, promised their customers with a high bandwidth availability and less than a quarter minutes of downtime per month, and service provisioning will include transfer requests, new service requests, direct supply, billing information, fault management, and allow the customer to reduce their payment by a given percentage if that is not accomplished [16].

In line with the active environment in cloud computing, it is required nonstop monitoring on Quality of Service (QoS) features are necessary to enforce SLAs. The SLA is the only authorized agreement between the service provider and customer. Although cloud customers do not have access over the fundamental figuring resources, they do need to ensure the excellence, availability, reliability and performance of these resources when customers have migrated their core business functions into their entrusted cloud. In other words, it is vital for customers to obtain guarantees from providers on service delivery [17].

This SLA serves as a foundation between the customers and the providers to begin transactions. The QoS attributes act as a significant part of an SLA (such as response time and throughput). However significant changes in the agreement must to be closely supervised. Evaluating the quality of cloud providers approach from a security point of view is difficult, because many cloud providers will not expose their infrastructure and applications to their customers. Due to the complex nature of customer demands, a simple "measure and trigger" process may not work for SLA enforcement. Attention in designing SLA improves the trust and therefore can increase throughput from the agreement.

SLA management is responsible for establishing, reviewing and cancelling of SLAs document with customer in all cases. In additional, the SLAs are based on service designs negotiated and agreed with the customer. Furthermore, the SLA is part of service delivery processes of International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 20000 standard [18].

ISO/IEC 20000 is an international Information Technology (IT) standard that allows companies to demonstrate excellence and show best practice in IT management. This standard ensures companies to achieve evidence-based benchmarks to continuously improve their provision of IT services. ISO/IEC 20000 was established in 2005 based on the IT Infrastructure Library (ITIL) best practice framework, and got updated in 2011.

The implementation of ISO/IEC 20000 has grown quite fast in the international field of IT service providers and it has become a competitive differentiator for supply IT services [19].

5) *Software and Hardware:*

Software and Hardware are a set of applications, programs, machines and virtual machines which is designed and developed to work together to perform the new technology in the business markets. Cloud computing offers software and hardware as services in the cloud. So basically the machines can't work without a program or software to on/and off the system or to input/ and output the data.

The physical devices that an individual able to touch it (tangible) is called hardware. And software is a set of commands collection, codes and instructions installed into the hardware device and cannot be touched (intangible). For instance, the individual is using keyboard in the computer to write any tasks in Microsoft word application and save it in computer hard disk. The keyboard is a hardware and Microsoft application is a software. Another example, the firewall device which is used in LAN and WAN network is a hardware, and the applications which are running inside the firewall device is the software [20]. Individuals or organizations need to assure that their devices comply with their security policies.

SEEK DIGITAL LIBRARY

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-69

Apart of hardware and software, the big companies allow their staff to use (BYOD) Bring Your Own Device technology. This technology lets users to carry their own devices anywhere they want in the company, but also they must follow the (BYOD) security policy[21].

6) *Organization:*

The organization can be defined as a community, or society or institute representing certain types of people, those people are working together to achieve the organization goal. The three layers of trust in any organization are as the following [22]:

- *Individuals level*, the trust is based on interpersonal interaction.
- *Groups level*, the trust is representing collective values and identities.
- *And System level*, the trust is institutional and based on systems, reputation and roles from which inferences are towed the trustworthiness of an individual.

The organizations and companies who are raising and cherishing trust as an important value in their work culture and working to build trust relationship behaviors between every individual in the organization is a successful organization[23]. But some organizations are weak when it comes to trust relationship in their work environment. So these companies are looking for ways to enhance the trust between individuals in their organization [24], and here are three steps to begin with:

6.1) ***Sharing Information,*** is one of the power and best ways to build trust between individuals. Sharing information can be by disclosing information and data that is considered privileged including sensitive and important subjects such as future plans and strategies of the organization.

6.2) ***Telling It Straight,*** the best quality in the leader and management is their integrity, the individuals who are working in any organization want always to follow someone they trust who will tell it straight. All these attributes mentioned needed to develop the trust essential for strong long term relationships inside and outside the organization.

6.3) ***Admitting Mistakes,*** leaders who admit mistakes when they are wrong are not seen as weak actually they are seen as having integrity and being trustworthy.

At the end of this part, we conclude that the trust in organization must be treated as valuable, highly appreciated, and a precious trait. The foundation of all strong and healthy relationships in organization are building trust relationship between managers and employees.

After we explained the elements of CCTRM model in details; we became able to identify that we can get the trust in each element, and we can get trust relationship if we achieve all the elements. This trust relationship can be between individuals or organizations. In section (IV) we discuss the overview of proposed CCTRM model.

IV. Overview of proposed CCTRM model

To enhance security and privacy in cloud computing environment, we proposed the trust relationship CCTRM model. This logical model can be used in any organization seeking for achieving trust relationship in their infrastructure environment. The main purpose of CCTRM model is to build trust between CSP and customers/ organizations. Figure (3) shows the process of CCTRM model.

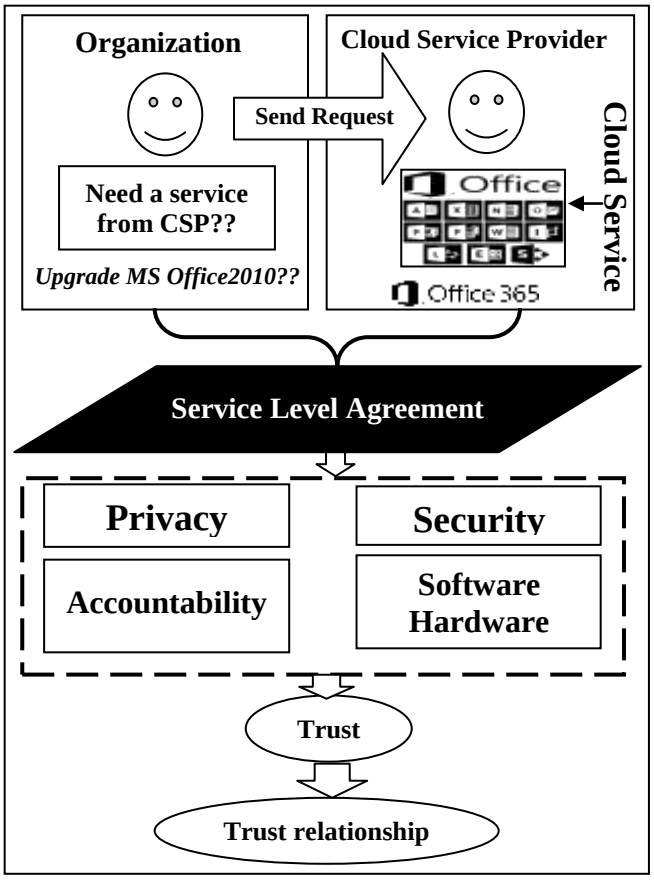


Figure 3. CCTRM model process

CCTRM model works when the organization sends a request for joining and getting a new service in the cloud from CSP. But before that the organization and CSP should agree about SLA. The SLA must provide privacy, accountability, security, software and hardware to the organization. Trust factor should be between two parties (organization and CSP).
If the two parties agreed then trust relationship will establish between them. The example in figure (3) shows that the organization has requested an upgrade for their Microsoft

SEEK DIGITAL LIBRARY

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-69

office (MS) set. They want to upgrade their MS office from 2010 to Office 2012 and join it to Office 365 in the cloud.
The organization agreed with CSP and they sign up the SLA; at the end they achieved all the element in CCTRM and they establish trust relationship.
In section (V) we will discuss case study for implementing CCTRM model in any organization.

V. Case study for implementing CCTRM model in organization infrastructure

Local organizations plan to transform their infrastructure and to reduce their operating costs by implementing (IAAS) private cloud. First the organization needs to agree and work with an CSP to understand the terms and conditions for SLA documents.
The organizations are looking to upgrade from windows server 2003 R2 and windows server 2008 R2 to windows server 2012 R2 with Hyper-V and to deploy the Microsoft System Center Suite of Products (MSCSP). Moreover, the organization planning to upgrade their mail server from Linux to Microsoft Exchange server 2013 SP1. And finaly join the organization to cloud environments.

A. *Overview of organization infrastructure*

This local organization is based on Kingdom of Bahrain since 2003 and its specialized in providing IT solutions and consultants for local companies who are looking to establish new business in information technology sector, and there are around 60 employees working at this organization.

Currently the organization is running a mixture of windows server 2003 R2 and windows server 2008 R2, the Operating System (OS) used are Microsoft windows 7 professional and the Microsoft Office set is Office 2003. This organization running Linux mail server and OS for mail server is red hat.

B. *Business need for improving infrastructure*

One of the main reasons push the organization to upgrade and change their infrastructure is the issues which they were facing it with Linux mail server such as sending e-mails, it always request the outgoing server Simple Mail Transfer Protocol (SMTP) authentication, and for every new employee it requires to create a user name and password, then it requests to setup Internet e-mail setting such as configure Incoming server port Post Office Protocol 3 (POP3) and Outgoing server port SMTP. This configuration takes time. So the organization decided migrate their Linux mail server with Microsoft Exchange and upgrade their Microsoft Windows Server to Windows Server 2012 R2 Standard, and upgrade Microsoft Office set to Microsoft Office Professional 2013.
The organization had a meeting with CSP, and they offered to do the work.
At this point the organization and CSP will have a work relationship until the project of improving the infrastructure is done.

C. *Solution*

The organization considered using virtual machines for their implementation, and found CSP (Microsoft) more competitive on price and offering easy integration, and strong security. The organization deployed Microsoft Center Data Protection Manager (MCDPM) 2010 to enhance organization infrastructure security. And migrated mail server with new Microsoft Exchange server, then they upgraded Microsoft OS for windows server to 2012 R2 along with Hyper-V virtualization technology to make use of agreement for low-cost volume licensing of software. On the Windows server 2012 R2 platform the organization implemented the MSCSP including Microsoft system center virtual machine manager 2012 R2 for improved data center management and performance monitoring. In additional, the OS of Windows Microsoft upgraded to Windows 8 and upgraded Microsoft office set to 2013 professional.
Finally, the SLA between organization and CSP (Microsoft) has included all the CCTRM elements (organization, SLA, security, privacy, accountability, software and hardware).

D. *Benefits of implementing the project*

Choosing the right CSP facilitate collaboration between the organization and CSP to trust each other and work smoothly. The CCTRM model achieved at this project and the benefits are listed below:

- The organization got a new environment sustainability for private cloud,
- This project helped to reduce operating costs from 100 percent to 50 percent,
- Improved manageability from the system center suite to all the products,
- Increased security part in organization infrastructure,
- Reduced physical servers from 20 physical servers to 10 physical serves, and that's allow to increase virtual servers,
- And, It became easy for technical teams to create and configure any new e-mail with Microsoft Exchange server.

VI. Conclusions and Future Work

Cloud computing has main security issues. In this paper we proposed CCTRM model to enhance security and privacy in cloud computing environment and to establish a trust relationship between CSP and organization. We choose a local organization and CSP to implement prototype of this model. And we succeeded in implementing model prototype. Our future work will be in implementing the CCTRM in real phase

SEEK DIGITAL LIBRARY

Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-69

and adding quality of service as new element to the CCTRM model.

VII. References

[1] N. Santos, K. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing*", In Proc.* the 2009 conference on Hot topics in cloud computing (HotCloud'09), Berkeley, pp.1-5 (Article 3) , June 15 ,2009

[2] W. FAN, S. Yang, J. Pei, and H. Luo, "Building trust into cloud", International Journal of Cloud Computing and Services Science (IJ-CLOSER), Vol. 1, No. 3, pp. 115-122, August 2012.

[3] S. Pearson, "Privacy, Security and Trust in Cloud Computing", HP Laboratories, (HPL-2012-80R1), pp. 1-57, June 28, 2012.

[4] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing", HP Laboratories, (HPL-2012-80R1), pp. 1-8, June 22, 2011.

[5] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", *In Proc.* the 2009 First International Conference on (CloudCom '09), China, pp. 69-79, December 1-4, 2009.

[6] X. Sun, G. Chang, and F. Li, "A Trust Management Model to Enhance Security of Cloud Computing Environments", *In Proc.* The second international conference on Networking and Distributed Computing (ICNDC'11), Beijing, pp. 244-248, September 21- 24, 2011.

[7] T. Mather, S. Kumaraswwamy, and S. Latif, "Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance", California, O'Reilly Media, 2009.

[8] B. Halpert, "Auditing Cloud Computing A Security and Privacy Guide", New Jersey, John Wiley & Sons, 2011.

[9] S. Pearson, "Toward Accountability in the Cloud", IEEE Internet Computing, IEEE Computer Society, vol. 15, no. 4, pp. 64-69, July-August 2011".

[10] S. Harris, "All in one CISSP Exam Guide sixth edition", McGraw-Hill, New York, 2013.

[11] S. Ahuja, and B. Moore, "A Survey of Cloud Computing and Social Networks", Network and Communication Technologies Journal, Vol. 2, No. 2, October 2013.

[12] K. Chard, S. Caton, O. Rana, and K . Bubendorfer, "Social cloud: Cloud computing in social networks." *Proc. IEEE 3rd Int. Conf. on Cloud Computing*, pp. 99–106, 2010.

[13] D. Marinescu, "Cloud Computing Theory and Practice", Elsevier Inc., Waltham, 2013.

[14] W. Stallings, "Computer security principles and practice second edition", Pearson Prentice hall, New Jersey, 2012.

[15] J. Daniell, A. Vervaeck, and F. Wenzel, "A timeline of the Socio-economic effects of the 2011 Tohoku Earthquake with emphasis on the development of a new worldwide rapid earthquake loss estimation procedure", *In Proc.* the 2011 Australian Earthquake Engineering Society Conference (AEES'11), South Australia, pp. 1-14, Nov 1-4,18-20, 2011.

[16] CIO Magazine on-Line, "SLA Definitions and Solutions", June, 2009, http://www.cio.com/article/128900/SLA_Definitions_and_Solutions?page=1#what .

[17] D. Al-Tehmazi, D. Nayak, M. Butt, M. Zaman, "Empowering Cloud Security Through SLA", Journal of Global Research in Computer Science, Vol 4, No. 1, PP. 30-33, January 2013.

[18] ISO Standers, " Certification to ISO management system standers", available in: http://www.iso.org/iso/home/standards/certification.htm

[19] ISO/IEC 20000 Organizational Certification Scheme available in: http://www.isoiec20000certification.com/

[20] J. Brien, and G. Marakas, "Management Information System Tenth Edition", McGraw-Hill, New York, 2011.

[21] L. Phifer, "BYOD security strategies: Balancing BYOD risks and rewards", Jan 28, 2013, http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards .

[22] A. Puusa, and U. Tolvanen, "Organizational Identity and Trust", Vol. 11, No. 2, PP. 29-33, 2006.

[23] The Ken Blanchard Companies, "Building Trust", 2010, online in: http://www.kenblanchard.com/img/pub/Blanchard-Building-Trust.pdf

[24] G. Tony, "Understanding Organizations – Part 1", Ventus , London, 2010.

SEEK DIGITAL LIBRARY