ISSN: 1991-8941

Trusted Cloud Computing

Sufyan T. Faraj * Waleed K. Awad* Kashif Kifayat **
University of Anbar - College of Computer
LJMU - School of Comp. & Math.Liverpool, UK .

Abstract: Cloud computing is a new consumption and delivery model for IT services. The cloud has become an attractive platform for enterprises to deploy and execute their business services for business to business (B2B) and government to government (G2G) collaborations, etc. There are many concerns about cloud computing especially in terms of security, privacy and trust. These main issues have prevented businesses from fully accepting cloud platforms. Cloud computing demands three primary security requirements: confidentiality, integrity, and availability. In this paper we discuss some these issues by reviewing a recently proposed model [1] that interestingly handles secure messaging among services deployed within the same cloud or on different clouds. Then, we report on our ongoing work which is based on enhancing and developing this model. This is mainly achieved by adding a new service layer which is responsible for offering a high level of trust between collaborative parties. The added layer facilitates the integration of this model with the Public-Key Infrastructure (PKI). The main objective of the developed model is to increase the trust of the whole system by preventing any unauthorized party from joining the connectivity service. Indeed, our system can prevent any involved organization from launching masquerade attacks.

Keywords-authentication service; Business to Business; cloud computing; PKI; security; trust

INTRODUCTION

Cloud computing can be considered as one of the latest developments in the Internet. No one really yet knows exactly where it is going or what the cloud will cover. It is expected that users will rent applications, software, and others as a services. Clients will not need to have computer with special properties such as (sophisticated hardware, minimal OS, etc.) because the processing power and storage will move from client hardware to centralized infrastructures. Many users, enterprises and other organizations will not need to store and operate large amounts of data. Using cloud computing users, enterprises, other organizations, and even governments can store and operate this huge amount of data in the cloud. Cloud providers can provide unlimited storage (e.g. S3) and parallel computing resources (e.g. EC2) [2].

While sharing IT infrastructure in cloud computing is cost-efficient and provides more flexibility for the clients, it introduces security risks organizations have to deal with. This is necessary so that they can isolate their data from other cloud clients and to fulfill confidentiality and integrity demands. Moreover, since the IT infrastructure well be under control of the cloud provider, the customer has not only to trust the security mechanisms and configuration of the cloud provider, but also the cloud provider itself. In general, important requirements of cloud clients are that their data is processed in a confidential way (confidentiality), and that their data and computation is processed in the expected way and has not been tampered with (integrity and verifiability). Secure outsourcing of arbitrary computation and data storage is particularly difficult to fulfill if a cloud client does not trust the cloud provider at all [3].

Voas and Zhang [4] discussed that there have been six main phases of computing paradigms, from dummy terminals/mainframe, to PCs, networking computing, to grid and cloud computing. In phase 1, many users shared powerful mainframe using dummy terminals. In phase 2, stand-alone PCs became powerful enough to meet the majority of user’s needs. In phase 3, PCs, laptops and servers were connected together through local networks to share resources and increase performance. In phase 4, local networks were connected to other local networks forming a global network such as the Internet to utilize remote applications and resources. In phase 5, grid computing provided shared computing power and storage through a distributed computing system. In phase 6, cloud computing further provides shared resources on the Internet in a scalable and simple way.

Comparing these six computing paradigms, it looks like that cloud computing is a return to the original mainframe computing paradigm. However, these two paradigms have several important differences. The most important difference is that mainframe computing offers finite computing power, while cloud computing provides almost infinite power and capacity. In addition, in mainframe computing dummy terminals acted as user interface devices, while in cloud computing powerful PCs can provide local computing power and cashing support [4].

Cloud Computing represents one of the most significant shifts in information technology that are likely to see fast growth. A Cloud can be viewed as a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources.

This work aims to effectively integrate the Public-Key Infrastructure (PKI) with a recently proposed (by Chen et al [1]) promising model of cloud computing in order to solve some of its important security concerns, and hence also to offer a high level of trust within this paradigm. This paper can be considered as a work-in-progress report on our work in this field. The remaining of this paper is organized as follows: Section 2 overviews some general concepts of cloud computing. Section 3 briefly discusses security and trust concerns of cloud computing. Then, the original Chen et al architecture is introduced in Section 4. In Section 5, some aspects of PKI and digital certificates are explained. Next, our proposed architecture for trusted e-contract based cloud computing is described in Section 6. Finally, Section 7 concludes the paper.

Cloud Computing Overview

A. Definition

There is not yet a consensus for what exactly the term "cloud computing" means; where everyone in the IT field defines cloud computing in different way. However, generally we can define cloud computing as a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access.

According to the U.S. National Institute of Standards and Technology (NIST), cloud computing can also be defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". [6]

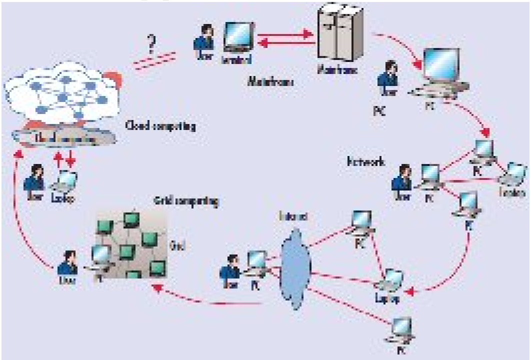

Figure1. Computing paradigm shift over six distinct phases [5]

B. Characteristics of cloud computing

There are many characteristics in cloud computing. Some of the most important of them are listed below [7].

- *On-demand:* Cloud computing provider must be able to deliver computing resources whenever the customer needs them. It is usually assumed that cloud contains infinite storage capacity for any software available in market. The available computing resources in cloud are nearly infinite (i.e., the customer is not limited to the set of servers located at one site and it is the responsibility of the cloud computing provider to have sufficient resources to satisfy the requirements of all their customers).
- *Pay-per-use:* Another new aspect of cloud computing is application of a usage based billing model. The customer pays only for use of processors or storage. That means the consumer does not need to large investment, license or paying software, etc.,

but the consumer can rent any services in efficient and rapid manner.

- *Maintenance and upgrading:* In cloud computing concept, the cloud provider maintains and updates all the computing resources whether the resource is hardware or software. That means the customer should not care to all problems such as maintenance, update, repairs and so on.
- *Rapid elasticity:* The amount of computer processing, storage and network bandwidth are available according to customer demand.

C. Cloud service models

Cloud Providers offer services that can be grouped into three major categories [7]:

- *Software as a Service (SaaS):* Software as a Service provides software applications as a service. Therefore, in the cloud users do not required to purchase the software rather the payment will be based on pay-per-use model.
- *Platform as a Service (PaaS):* Platform as a Service is a set of software and product development tools that allows building applications on the providers' platform. Here a layer of software or development environment provided as service.
- *Infrastructure as a Service (IaaS):* Infrastructure as a Service is a service delivery model in which an organization is given control over applications and resources like storage, servers, hardware, components. This model is similar to a utility company model, as you pay for what you use. Table 1 includes some available providers according to these three service models.

Table 1. Major Providers of the Cloud Services

Service Type	Provider Name
SaaS	Saleceforce, Microsoft, Google Docs
PaaS	Google App Engine
IaaS	Amazon S3, Amazon EC2

D. Types of cloud computing

There are three main types of cloud computing namely private, public, and hybrid cloud computing. These three types are also called deployment models (See also Figure 2) [8].

- *Private cloud computing:* Private cloud computing resides within the boundaries of an organization and is used exclusively for the organization's benefits. Private cloud is similar to that of intranet. This type of cloud computing has more benefits with increased security, reliability, and corporate ownership of the cloud. The data and applications in an organization require a secure connection. By using the concept of cloud computing, private cloud computing has become a viable choice for the organizations to implement cloud computing. It is predicted that the future IT corporations would be greatly dependent on this type of cloud computing. Examples of private cloud are Microsoft's.
- *Public cloud computing:* Public cloud computing somewhat resembles internet where the access is available to public domain. Public clouds are administrated by third parties or vendors over the Internet, and services are offered on pay-per-use basis. This helps the users to create and use a service or application at a much lower cost when compared to the cost incurred in purchasing, installing, maintaining and licensing in individual computers. This is also called provider cloud. The examples for this type of cloud computing is Amazon Elastic compute cloud, Google app engine, and Windows Azure.
- *Hybrid cloud computing:* Hybrid cloud computing combines the features of both private and public cloud computing. Enterprises or organization need this type of environment because it cannot develop itself on private cloud alone and they might require the public cloud to meet various organizational demands.

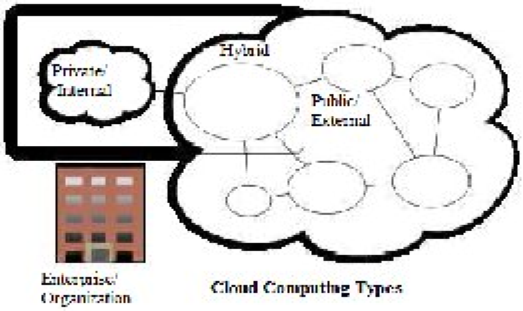

Figure 2. Types of Cloud Computing

CLOUD COMPUTING SECURITY ISSUES

Although, there are great benefits of cloud computing such as (ease of use, low cost, etc.). Cloud computing also have some disadvantages, the key challenges that related with cloud is security, privacy and trust. The top concern is the security needed to be addressed when considering moving critical applications and sensitive data to public cloud environments. Security in the Cloud is often intangible and less visible. The off-premises computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, where cloud service providers may have complete control on the computing infrastructure that underpins the services. Various security challenges that can be characterized as particular to cloud-computing context are [9]:

- Failures in Providers Security
- Attacks by other customer
- Security of third party access
- Availability and reliability issues
- Identity and access management
- Lack of security and quality levels

According to Cloud Security Alliance (CSA), the top seven security threats of cloud computing are [10]:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

As far as the paradigm of cloud computing is concerned, the issue of trust cannot be totally separated from the other two concerns of security and privacy. We believe that the right and proper deployment of some cryptographic techniques and other related security procedures will not only result in higher security and privacy levels, but will also significantly support building trust into cloud computing.

Related Cloud Computing Architecture

In [1], Chen et al presented architecture for secure communication in a cloud-based collaborative in B2B environment. They examined this issue by reviewing existing technologies. Then they presented an electronic contract (e-contract) based solution that provides a secure Connectivity as a Service (CaaS) for intra-cloud and inter-cloud communications with little configuration effort.

The interaction of components of this architecture (See Figure 3) starts from collaborating parties. At the beginning, each collaborator resides within its own administrative domain. To form an extranet for dynamic B2B collaboration, all collaborators (e.g., organizations A, B, and C in the figure) must subscribe to the offered Connectivity Service. Next, according to the nature of the collaboration, each organization can either invite (its business partners) or be invited to join a collaboration to form an extranet. Finally, an e-contract is formed and signed by each collaborating parties. The connectivity service can configure and instantiate an extranet as specified in the e-contract (e.g., Extranet 1 and Extranet 2 in Figure 3). Thus, the services deployed in clouds can communicate with each other within the extranet (e.g., Service A1 and Service B1 within Extranet 1 and Service A2 and Service C1 within Extranet 2) [1].

Connectivity Service can be considered as a trusted third party service provider for both intra-cloud and inter-cloud secure communication in order to demonstrate B2B collaboration through e-contracts (An e-contract simply is an agreement between two or more entities created and "signed" in electronic form [11]).

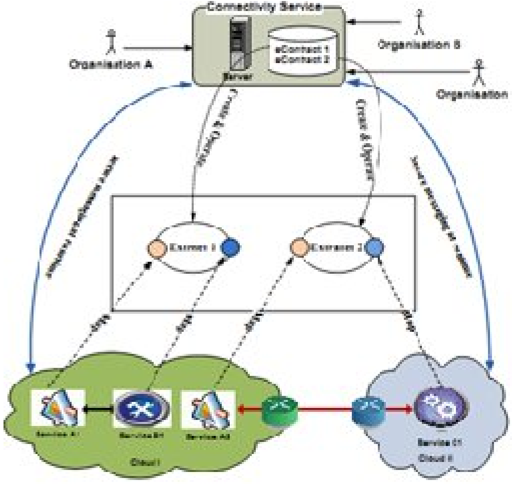

Figure 3. Architecture of e-contract based secure connectivity service

It can be noted that according to this model or architecture, in order to use the connectivity service, an organization needs first to join the service by invitation from another one (or by subscription for a more generalized framework). However, this system might suffer from serious attacks, when unreal (or unauthorized) organization attaches itself and threaten the whole system security. This case can decrease the trust value among the real organization.

Therefore, in this work, we are developing and enhancing the mentioned model by effectively integrating it with PKI. This can be considered as adding a new layer for trust which is responsible for detecting unreal organizations. Moreover, our enhancement will contribute to trust from other complimentary direction via preventing authorized or collaborated organization from launching masquerading attacks through the proper management of PKI certificates.

There is now a wide acceptance among security experts to use cryptographic signatures based on PKI. This can be considered as the most secure and reliable method of signing e-contracts online. The X.509 is a widely accepted standard for developing PKI-based authentication services. According to this standard, after the certificate is generated, the requirement of transmission needs the format of certificate to be changed into Abstract Syntax Notation One (ASN.1) binary file, which is a standard to be exchanged between communicating application programs [12]. More details about PKI certificates are in the following section.

PKI AND DIGITAL CERTIFICATES

PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money. This is basically done through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI provides for a digital certificate that can identify an individual or an organization. It also provides directory services that can store and, when necessary, revoke the certificates. PKI assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender and checking the integrity of a message [13].

Public key cryptography with its dual key system (public and private keys) seems to best solve the integrity, authentication, and non-repudiation requirements of open networks. It is more suitable when compared with the classic cryptographic methods. It gained more popularity in the Internet world because of its scalable tools for key management problems. The main problem in a symmetric key cryptosystem is its key-management problem where the same key is used to encrypt and decrypt the message. This secret key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted .Therefore the public key cryptosystems are presented as a solution to this problem with its dual-key system. In a public key cryptosystem, private keys are kept secret by their owners, while the corresponding public keys are stored in a public repository with the names of their owners [14].

PKI is the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke public key certificates based on public key cryptography" [13]. The basic components of PKI certification system are [14], [15], [16]:

1. *End-entities:* End-entities in a PKI can be human beings, devices or even software programs. The cryptographic operations (encryption, decryption and digital signature) are performed by the end-entities. In general, the end-user may request certificates from a certification authority (CA), receive the certificate from the CA, and then use the certified keys and certificates in PKI enabled application services.
2. *Certification Authority (CA):* It is also named trusted third party (TTP). CA is an entity in PKI, which is responsible for issuing and manage certificates for the other entities in the system and also checks with registration authority (RA) to verify the requestor's information. In the context of a PKI, certification is the act of binding the identity with a public key. This binding occurs in the form of a signed data structure referred as a certificate.
3. *Registration Authorities (RA):* RA is a component that is responsible to verify the identity of end-entities .It is possible to implement the necessary registration functions by a CA, but many PKI implementations separate the operations performed by the CA and the RA to avoid the complexity of tasks.
4. *Digital Certificates:* It is an electronic document which uses a digital signature to bind a public key with identity information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public

key belongs to an individual. It is also known public key certificate (PKC) or identity certificate. Digital certificates contain information such as public key, the entity owning this public key and a set of other attributes written in the certificate with a valid digital signature of the issuer. There are a lot of certificate types. Some of them are X.509 Public Key Certificates, Simple Public Key Certificates (SPKC), Pretty Good Privacy (PGP) Certificates, and Attribute Certificates. In this work we will adopted a version of X.509 public key certificates. Figure 4 illustrates the general structure of an X.509 v3 certificate.

5. *Certificate Repositories (CR):* A certificate repository, sometimes referred to as a certificate directory, it is an entity in PKI. To establish trust and/or secure communication, certificates should be available for anyone who needs them. CR could simply be posted on a public homepage, and put in a database. This is referred to as a repository.
6. *Certificate Policies (CP):* A certificate policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements.
7. *Certificate Practices Statement (CPS):* The certificate practice statement (CPS) translates certificate policies into operational procedures on the CA level. The certificate policy focuses on a certificate; the CPS focuses on a CA.

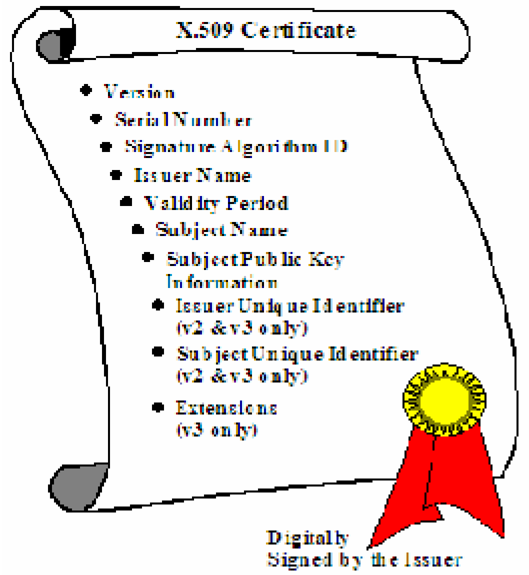
X.509 Certificate
Version
Serial Number
Signature Algorithm ID
Issuer Name
Validity Period
Subject Name
Subject Public Key Information
Issuer Unique Identifier (v2 &v3 only)
Subject Unique Identifier (v2 &v3 only)
Extensions (v3 only)
Digitally Signed by the Issuer

Figure 4. X.509 V3 certificate [12]

The Proposed System Architecture

Enabling trusted e-contract based collaboration between organizations in the cloud environments can be a significant application of B2B in cloud computing. Our proposed work is an enhancement of the Chen et al model [1] described previously. It can be noticed that in Chen et al model, in order to use connectivity service, the organization needs to join the service by invitation from another one (or by subscription for generalized case). Therefore this system might suffer from some attacks, where unreal organization can attach itself and threaten the system security. This case can decrease the trust value among real organizations. In addition, generalizing this work to enable reliable, secure, and trusted subscription of organizations requires additional upper layer work. Attacks from insiders (i.e. from organizations already involved in one or more e-contracts collaboration) are indeed another major concern of this earlier work.

Our proposed system model addresses all these problems and more by adding new upper service layer to the above model. This added layer is called Authentication Service layer (See Figure 5) and it is responsible to increase the trust value of the whole framework. This is mainly achieved by detecting and preventing unreal (or unauthorized) organizations that want to join the connectivity service, facilitating the prevention of masquerade attacks from insiders, and by offering the required platform for secure and reliable system subscription and log out. This functionality of the added layer depends on PKI-based digital certificates. Thus, a proper and efficient integration of the basic model of e-contract based collaboration with the PKI is needed. We have already completed the required architectural design and started implementing some of its basic components in an experimental private cloud environment.

The basic components of the added authentication service are:

- *Certificate Authority (CA):* It is in charge of generating certificates for organizations, i.e. signing an organization's public key and identity information with its own private key.
- *Registration Authority (RA):* It is in charge of verifying organization's identity and associating that identity with its public key.
- *Validation Authority (VA):* It is a validation system that can confirm whether a specific organization's certificate produced by this

CA is still valid or not (for example, because the associated private key was lost or compromised).

- *The End Users:* They are the organizations' representatives involved (or want to be involved) in the collaboration.

Figure 6 shows the basic interaction steps among these components with the client and the cloud service. These steps are as follows:

- *Step1:* Client (organization) sends identity to RA.
- *Step2:* RA checks client identity and other information using a set of roles stored in RA.
- *Step3:* RA sends positive acknowledgment (if everything is OK) and the required key to CA.
- *Step4:* CA sends the key and certificate to the client.
- *Step5:* CA also sends the key and certificate to the VA.
- *Step6:* Client sends request using the obtained key.
- *Step7:* Upon approval, VA communicates with the client using this key.

Of course, the above mentioned interaction steps have to be extended in different aspects in order to enable reliable and secure actions in the cloud. Detailed and proper protocol implementations are required to be achieved to take into account various possible threats in real cloud computing settings.

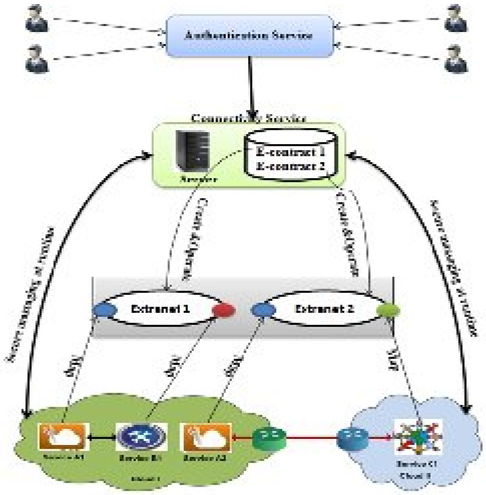

Figure 5. The general architecture of the enhanced system for e-contract based cloud computing collaboration

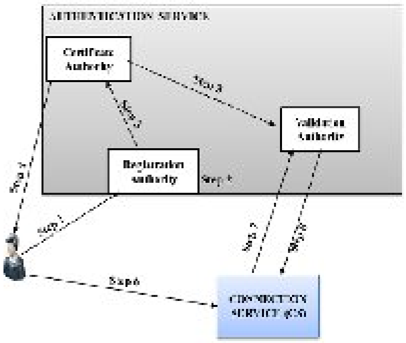

Figure 6. The basic interaction steps between entities for authentication service

Before integrating the main two parts of the proposed system (i.e. the connectivity service and the authentication service layers), we are working in parallel also to complete the basic engine for the e-contract based cloud computing collaboration. Among the require tools for this engine are the SSL-based VPNs (virtual Private Networks). Such VPNs can provide a secure connectivity for a group of collaborative services by forming a virtual extranet within a cloud and/or between Clouds. Following the Chen et al work, we are also working on developing three Amazon EC2 alike instances [17]. The first is for running OPEN VPN server v2.1 [18]. The second is for running a Web service deployed on Apache tomcat v6.0 [19]. The third is for running the Web service client. Java language is used for implementing the web service and client applications. After completing the integration of all parts of the system, a detailed evaluation study will be performed to assess the total level of trust offered by the whole framework.

CONCLUSION

Although that cloud computing gained a lot of reputation, but still there is concern about this concept throughout the world especially regarding its security environments. In order to make more organizations moves towards cloud computing, strong mechanisms and technologies are needed to be established such that to overcome the problems of security, privacy, and trust. In this paper, we have discussed security and trust issues by reviewing recently developed model that handles secure messaging and among collaborative services within the environment of cloud computing. We then described our development on this model by adding new service layer that is responsible to increase trust in such collaboration through proper integration with PKI. As our work in the development of this system is still in progress, we will try to deploy the best available security practices to prevent possible threats from outsiders and insiders. We believe that achieving this goal is necessary to build the required level of trust in cloud computing.

REFERENCES

[1] Shiping Chen, Surya Nepal, and Ren Ping Liu, "Secure Connectivity for Intra-cloud and Inter-cloud Communication," ICPP Workshops, 2011, pp. 154-159.

[2] Srinivasa Rao, Nageswara Rao, and Kusuma Kumari, "Cloud computing: An overview," Journal of Theoretical and Applied Information Technology, Vol.9, No.1, 2009.

[3] Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy,"Token-based cloud computing - Secure outsourcing of data and arbitrary computations with lower latency," 3rd International Conference on Trust and Trustworthy Computing (TRUST'10) - Workshop on Trust in the Cloud, June 22, Berlin, Germany.

[4] Jeffrey Voas and Jia Zhang, "Cloud computing new wine or just new bottle," Journal of IT Professional, Volume 11, Issue 2, March 2009.

[5] P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, 2009.

[6] VICTOR DELGADO, "Exploring the limits of cloud computing," Master of Science Thesis, Stockholm, Sweden 2010.

[7]. Jianfeng Yang and Zhibin Chen, "Cloud Computing Research and Security Issues," International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan, China December 2010, pp. 1-3.

[8]. Joe Nisha . "Cloud Computing – An overview on cloud computing concepts," India Study Channel, Posted on 06 Sep 2011.

[9] Pardeep Kumar, Vivek Kumar Sehgal , Durg Singh Chauhan, P. K. Gupta and Manoj Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing," IJCSI International Journal of Computer Science, May 2011.

[10] S. Srinivasamurthy, F. Wayne, and D. Q. Liu, "Survey on Cloud Computing Security," Computer, 2010 (available at http://salsahpc.indiana.edu/CloudCom2010/).

[11] http://en.wikipedia.org/wiki/elecetonic_contract.

[12]. W. Zhao, "Implementation of Software Tools for the Medium-Size Certification Authority _ X.509 Certificate", ECE Dept., George Mason University, December 2003.

[13]. http://en.wikipedia.org/wiki/ PKI (public key infrastructure).

[14] E. YILDIZ ,"A Proposal for Turkish Government Public Key Infrastructure Trust Model" , MSc Thesis, December 2001.

[15]. Sufyan T. F. Al-Janabi. and Amer Kais. "Development of Certificate Authority Services for Web Applications" The First International Conference on Future Communication Networks (ICFCN '2012), Baghdad, Iraq, April 2012 (Submitted).

[16] ITU-T Recommendation X.509, "The Directory: Public Key and Attribute Certificates Framework, 2000.

[17] Amazon EC2: http://aws.amazon.com/ec2/.

[18] OpenVPN: http://openvpn.net.

[19] Apache Tomcat: http://tomcat.apache.org/.

الحوسبة السحابية الموثوقة

سفيان تايه فرج وليد كريم عواد كاشف كفايات

E.mail: sufyantaih@ieee.org

الخلاصة

الحوسبة السحابية نموذج جديد للاستهلاك والتسليم لخدمات تكنلوجيا المعلومات. الحوسبة اصبحت بيئة جذابة للشركات او الحكومات لنشر وتنفيذا اعمالهم للتعاونات سواء كانت (B2B) او (G2G).الخ. هناك العديد من المخاوف حول الحوسبة السحابية ولا سيما من حيث الامن والسرية والثقة.وقد منعت هذة القضايا الرئيسية الشركات من قبول منصات الحوسبة السحابية بشكل كامل. تتطلب الحوسبة السحابية ثلاث متطلبات امن رئيسية: السرية, التكاملية والاتاحية. في هذا البحث ناقشنا بعض هذه القضايا من خلال استعراض نموذج تم اقترحه مؤخرا والذي يعالج الارسال الامن بين الخدمات المنتشرة ضمن نفس السحابة او على سحابات مختلفة.ثم, نذكر بعملنا المستمر على والذي يستند على تحسين وتطوير هذا النموذج. ويتحقق هذا بأضافة طبقة الخدمة جديدة والتي تكون مسؤولة عن تقديم مستوى عال من الثقة بين الاطراف التعاونية. الطبقة المضافة تسهل تكامل هذا النموذج مع البنية التحتية للمفتاح المعلن (PKI). الهدف الرئيسي للنموذج المطور هو زيادة ثقة النظام بالكامل بمنع اي كيان غير مخول من الانضمام الى خدمة الربط. في الحقيقة, نظمنايمكن ان يمنع اي منظمة معنية من اطلاق هجمات التنكر.