IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 2) Pages (126-139)

Journal home page: www.ijreb.org

ENHANCING SECURITY IN TRUST AWARE IDM FOR CONSUMER CLOUD COMPUTING

Anjisha R

Dept. Of Computer Science, TKM Institute of Technology, Kollam, India

ABSTRACT

Consumer cloud computing is an important area of interest in the field of cloud Computing. In the consumer cloud environment the major attention is focused to the distribution of information and heterogeneity of clouds security and identity management challenges. In this paper, the problem of file security and secure keyword search over encrypted outsourced cloud data is reduced with the help of IdM Architecture. Ranked search greatly enhances system usability by enabling search result in relevance with the file retrieval accuracy. An Advanced Encryption Standard (AES) is used to provide the user, only the necessary information and distributing the key of those attributes for proper authentication of the clients.

KEYWORDS: Identity Management, Dynamic Trust Management, Privacy, Consumer Cloud Computing.

INTRODUCTION

Cloud Computing is a type of computing infrastructure that consists of a collection of inter-connected hardware such as nodes, servers etc as well as software services.The applications are dynamically provisioned among users. The Cloud Services are distributed over the Internet or private networks, or in the combination of networks. The cloud services are accessed over these networks based on their availability, performance and capability requirements. It mainly focus to issue secure, reliable, sustainable and scalable services, to the end-users. These systems have goals of providing virtually unlimited computing and storage and hiding the complexity of large-scale distributed computing from users. Thus cloud computing is a new way to deliver computer resources.

The consumer cloud computing platform is a networked collection of servers, storage systems, and devices in order to combine software, data, and computing power scattered in multiple locations across the network. Consumer cloud computing offers resources as services that are more flexible, scalable, affordable and attractive to customers and technology investors. Thus consumer cloud computing enables different applications related to consumer electronics (CE), such as virtualization of consumer storage, Cloud TV platforms that provide access to a number of Web applications such as social networking, user generated video games, etc[1].

Identity management (IdM) is defined as an integrated concept of process, policies and technologies that enables authoritative source to accurately identify entities and control the use of information between them. Identities corresponds to the entities and consisting of attributes and identifiers. Identity management is the task of controlling information about users on computers. Such information includes information that authenticates the identity of a user, information that describes information and actions they are authorized to access and/or perform. It also includes the management of descriptive information about the user and how and by whom that information can be accessed and modified. Managed entities typically include users, hardware and network resources and even applications.

In this paper, a dynamic security-enhanced federated identity management solution for cooperation, on demand resources provisioning and delegation in cloud computing scenarios, preserving the user's files and secure search for their files. This proposal extends an enhanced security module in order to provide an efficient identity management and access control, as well as dynamic, autonomic, and user-centric establishment of cloud federations An enhanced IdM architecture which can be used in any cloud applications is developed.

This paper is organized as follows: in section II, we give an overview about related work. Section III provides a brief description on identity management in consumer cloud computing. Then, section IV describes the proposed architecture and details the core components. Section V explains Security Management and VI explain the implementation details. Finally, Section VII summarizes the presented work and some future lines.

RELATED WORK

This section covers the technologies and methodologies about IdM in consumer cloud computing, focused on identity management, dynamic federation, security and search issues. The proposals mentioned are specially centred in cloud computing, because cloud computing in consumer electronics is still an evolving paradigm. So, our proposal considers aspects as multiple factor authentication, user control, portability and personalization while respecting user's privacy.

A. Identity management in cloud computing

Even though there have been many advancements in fields of authentication and authorization using user-centric approach in the areas of media sharing, cloud services, and personal content none of them deals with dynamic federated identity management. The paper [18] provides a methodology of authentication in consumer electronic devices, by giving the permissions to the user to share their content rights and services in secure and trusted environments, temporarily. The zero-knowledge proof methodology preserves user's privacy while providing him his identity. But, dynamism in trust relationship management is not addressed in this process. For virtual machine user authentication, Zero-knowledge proof techniques can be used as given in [19]. It proposes an active bundle scheme called IdM wallet, for securing personal user information from untrusted parties, using entity-centric model. This paper addresses issues like trust and privacy using trust evaluation model and audit services model.

B. Dynamic federation between cloud providers

Though being realised as a crucial link in usability and scalability, my important aspects are still to be addressed in dynamic trust establishment. Though In [20] a SAML based three-phase cross-cloud federation agent technologies and model is proposed, but establishment of trust between unknown parties is not given. Also, the developing next generation computer application is the base for distributed environment trust management peer to- peer systems [21]. In the technique [22] trust values are found based on personal dependencies in a community using reputation based on local and global scope.

C. Confidentiality

Confidentiality management is an important for aspects, client's trust and legislation when he tries to access consumer cloud computing. While legislation in different geography may have different rules, but broad privacy principles specified in [23] are applicable in most parts. The author has given many suggestions and techniques to make a privacy aware IdM architecture like specifying and limiting the usage of user data and reducing the amount of information sent to and stored in the cloud, allowing user choice, maximizing user control, providing the customer with privacy feedback and protecting sensitive customer information. In [19] many principles are used for managing the disclosure of identities. Also, for mitigating issues like frauds, identity misuse, unauthorized access to personal data etc and consumer cloud scenarios, Fair Information Principles [24] can be applied. Second issue to be addressed is the cross-site sharing and tracking of data collection mainly used by advertising or personalization. Using this track data stored at a trusted cloud provider can invoke doubt in user. Federal Trade Commission [25] has pointed out the user's right to opt out of Web tracking. Hence, we can say that still many issues on privacy in consumer cloud that are needed to be addressed. In cloud scenario, critical privacy issues demands the need for faithful digital identity infrastructure which is nicely pointed out by the author in [26]. Also, in [27] we can find a fine example on preserving user's privacy in consumer electronics and how cloud computing technologies can help in it. It gives a technique to maintain user's privacy while exchanging EHR in a cloud platform, but access issues to this data and not fully addressed.

D. Existing identity management tools

Some known identity management tools are as follows:

Privacy and Identity Management for Europe

Privacy and Identity Management for Europe (PRIME) provides privacy- preserving authentication using anonymous credentials. The user-side component uses protocols for getting third party (IdP) endorsements for claims to relying parties (RPs). Anonymous credentials are provided using an identity mixer protocol (based on the selective disclosure protocol) that allows users to selectively reveal any of their attributes in credentials obtained from IdP, without revealing any of their information. The credentials are then digitally signed using a public key infrastructure. A major limitation of PRIME is that it requires both user agents and SPs to implement the PRIME middleware, which hinders standardization.

Windows Card Space

Windows Card Space is a plug-in for Internet Explorer 7, in which every digital identity is a security token. A security token consists of a set of claims, such as a username, user‗s full name, address, SSN etc. The tokens prove that the claims belong to the user who is presenting them. The Card Space framework is criticized due to its reliance on the user‗s judgment of the trustworthiness of an (Relying Party) RP. Most users do not pay attention when asked to approve a digital certificate of an RP, either because they do not understand the importance of the approval decision or because they know that they must approve the certificate in order to get access to a particular website. RPs without any certificates at all can be used in the Card Space framework (given user consent). Even if an RP presents a higher assurance certificate, the user still needs to rely on an IdP providing that certificate to the RP, thus the user needs to trust the IdP. Another drawback is that, in a case where a single IdP and multiple RPs are involved in a single working session, (which we expect to be a typical scenario) the security identity meta system within the session will rely on a single layer of authentication, that is, the authentication of the user to the IdP. If a working session is hijacked or the password is cracked the security of the entire system is compromised.

Open ID

OpenID is an open, decentralized, free framework for user centric digital identity management. It takes advantage of already existing internet technology and realizes that people are already creating identities for themselves whether it be at their blog, photo stream, profile page, etc. They can easily transform existing URLs into an account which can be used at sites which support OpenID logins. Its major advantages of are:

- Highly distributed
- Flexible – users can keep identity even when identity provider disappears
- Lightweight solution

OpenID has been termed ―phishing heaven due to its susceptibility to phishing attacks and social engineering. A malicious attack can be easily set up to lure users into entering their authentication information at a website that poses as an OpenID provider website.

Higgins

Higgins is an open-source framework and collaborative project which among other things develops components that can be used to build the different parts of an identity management system. There are two major categories of Higgins components (1) Lower-level components can be used to create identity services such as attribute services, token services and relying party Web-sites and services. Upper level components can be used to create user-centric applications which allow the user to view, employ and manage his/her various identities (i-cards).More specifically, (2) Higgins‗ upper-level components can be used to build identity agents which allow users to accept i-cards from card issuing sites (i.e., identity providers), they can be used to create self-issued cards, manage a user‗s set of cards and to use these cards towards service providers (relying parties) or local applications.

Liberty Alliance

Liberty Alliance specifies open standards for identity management. The specifications define sets of protocols that collectively provide solutions for identity federation management, cross-domain authentication and session management. The specifications also define provider metadata schemas that may be used for making a priori arrangements between providers. The Liberty architecture contains three actors: Principal (the end user), identity provider (IdP) and service provider (SP). The Principal has an identity provided by an IdP. A SP provides services to the Principal. Once the Principal is authenticated to the identity provider, the IdP can provide an authentication assertion to the Principal, who can present the assertion to the SP. The Principal is then also authenticated to the service provider if the SP trusts the assertion. An identity federation is said to exist between an identity provider and a service provider when the service provider accepts authentication assertions regarding a particular Principal from the identity provider.

CURRENT IdM ARCHITECTURE

The current IdM infrastructure has the functionality to allow Identity Providers (IdPs), Service Providers (SPs), and enhanced clients to share common knowledge. The ECP (Enhanced Client Profile) has been defined especially for consumer cloud computing. This ECP gives the required user-centric approach needed for consumer electronics.

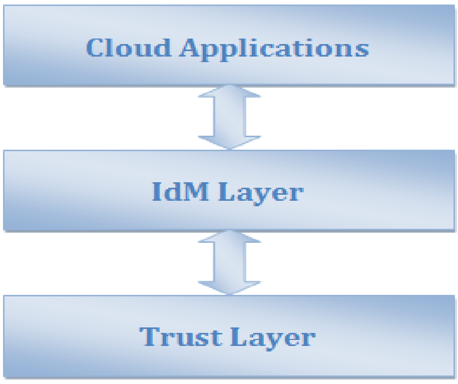

Fig. 1: Layered Architecture for ECP.

The ECP is a software element which minimizes direct interactions between SPs and IdPs, and provides full control to users over their identities, thereby improving mainly privacy. The layered architecture for ECP is shown in figure 1.

At the top of the architecture for CSP/IdP or ECP there is the Cloud or the Apps layers. The first one contains cloud services offered by cloud providers (SPs or IdPs). The second one is located on the ECPs, containing client applications. The second layer is the IdM layer, which gives the basic functionality of each role defined in the SAMLv2 specification. In addition, such basic functionality is extended by adding the Privacy Engine module. Finally, there is the Trust layer, focusing on the reputation manager in order to allow secure interaction between unknown parties. This last layer combines reputation information with other related data, for instance, historical interactions. So the user can request access, through the ECP installed on his mobile, to services provided by SPs and IdPs. Trust Layer calculates the trust value of interaction betwwen the users and the service providers. IdM Layer includes various components to perform different functions as shown in the fig. 2.

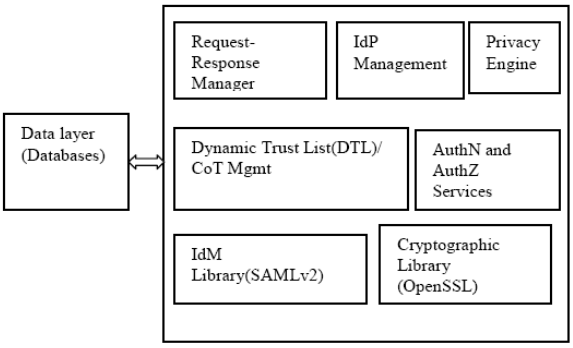

Fig. 2: Components of IdM Layer.

Proposed Architecture

The concept of identity management basically aims at providing a common knowledge to service provider's (SP's), identity providers (IdP's) and the enhanced client. The architecture for security enhanced IdM is shown in the fig. 3. The entire architecture includes different modules as given below:

Request-Response Manager:- This module receives authentication, authorization or attribute requests from the applications. This module provides the interface between AuthN and AuthZ Service and applications. These requests can be initiated by authentication request statements from the SP.

AuthN and AuthZ Service Management: - The function of this module depends on its location. So, it receives and processes the <AuthnRequest> messages from either the SP or the ECP, regarding to the ECP or IdP, respectively. In the CSP, it issues such authentication and authorization request. The modules in each unit i.e. either in ECP, IdP, CSP interacts to verify the user requesting a service is really who he claims. For this purpose, it supports multiple authentication mechanisms including PKI, username/password, etc. For authorization process, the security assertions and the attributes exchanged informs about authentication decisions, profiles and attributes to cloud services providers which help them to decide what services or resources the user can access. For that, this module issues (IdP) or verifies (SP), and manages SAML authentication assertions and attribute statements. The aim is to assist authentication and user management to users and cloud services. Thus, improving the users' experience by reducing complexity and management costs.

Identity Management: - This module coordinates with the DTL/CoT Management and the trust layer to configure trust relationships with the IdPs in a dynamic and secure manner. Also, it is responsible for determining the most satisfactory identity provider depending on the requested service, the user's preferences related to privacy and security and the context. For example, in some contexts the user may not want to disclose any personal information, whereas in other contexts he may wish for partial or full disclosure of identity. To accomplish these tasks, this module collaborates with the Request-Response Manager and the Privacy and Security.

Dynamic Trust List (DTL)/CoT Management:-The function of this module is to maintain an Updated circle of trust, which contains more complete information than traditional certificate lists, such as trust level, previous interaction results, reputation scores, keys, etc. This trust information is automatically updated through modules in the Trust layer.

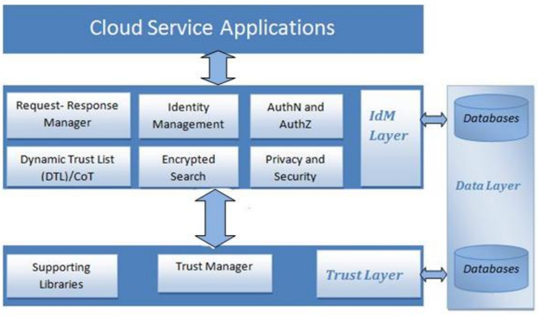

Fig.3: Security Enhanced IdM Architecture.

Encrypted Search: - The function of the module is to receive the request from the applications and retrieve files based on the request. An efficient rank ordered search over the encrypted files in the cloud data helps to retrieve the files very easily and accurately.

Privacy and Security: - This module mainly focuses on the privacy of the users' credentials and security of the users' files. These modules are supported by basic libraries such as IdM and cryptographic, which implement SAMLv2/ID-FF functionalities and cryptographic algorithms and protocols, respectively. In the user's side, these libraries implement the minimal functionality, taking into account limited devices.

Supporting Libraries: - Basic supporting libraries like IdM and cryptographic implementing SAMLv2/ID-ff functionalities and cryptographic protocols and algorithm are also included. A light version of these libraries is also included in the user's side.

Trust Manager: - It organizes the communications and operations of the described modules, and manages the trust data repository. It is responsible for managing dynamically trust information, negotiating the trust relationship establishment, and providing trust data to other layers. The trust information contains data related to the entities' behaviour and external trust information from trusted third parties, thus it takes advantage of the common knowledge in the federation. Finally, the TM is also augmented with more complex functionality, such as context and policy management for making richer decisions depending on the actions defined by policies and context in each specific situation.

Dynamic federation establishment

Reputation can be considered as a collective measure of trustworthiness based on the referrals or ratings from members in a community [1]. Adding reputation support to SAML implies modifications to both Assertions and Protocols. Here a new assertion is defined. Such assertion is a custom statement type, called [1] <Reputation Statement>, which is conveyed in a response message. The structure of such reputation assertion has an initial part (i.e. header), whose content is the same defined in the standard. This common section includes the assertion identifier (ID), the names of the issuer and the subject, and information about the instant in which the assertion was issued. The <Subject> tag, in our case, indicates the identifier of the entity for which reputation data has been requested. Apart from this information, the statement contains a body section, which contains all the related data to the reputation metric. These include the following attributes:

- Reputation Instant, to ensure data freshness;
- Reputation Score that corresponds to the reputation value;
- Distribution Function, for the reputation to be aggregately;
- Context, to illustrate for what situation the reputation was made.

This <Reputation Statement> is exchanged using the SAML "Assertion Query and Request Protocol". So query/response formats are as per the rules defined. The communication flow has the following steps:

1. A user accesses a service offered by a CSP2. The CSP2 needs to authenticate the user, so it performs IdP discovery for determining who should be asked for user authentication. This checks local configuration data to see if the discovered IdP is known.

2. As CSP2 determines IdP1 is unknown, the RM executes the logic to gather reputation information about it. This sends a <Reputation Request> acting as a Reputation Requester.

3.The IdP2 and CSP1 returns a <Reputation Response> containing a

<Reputation Statement> in case of success, or an error message in case of failure. These entities would be a Reputation Responder. As IdP1 is trusted in accordance with the reputation information received, then the CSP2 downloads IdP1 metadata and initiates SSO as usually.

4. The CSP2 requests user's authentication to IdP1.

5. IdP1 authenticates user and sends the successful authentication response to the CSP2.

6. Finally, the CSP2 grants service access to user. Here the aim is to demonstrate that collecting external information allows flawless trust establishment and facilitates this kind of interactions, otherwise impossible or insecure. We have worked with a simple SAML-based SSO scenario: a user, two CSPs, and two IdPs. In this situation, CSP2 and IdP1 are unknown, so CSP2 requests information about IdP1 to trusted providers such as IdP2 and CSP1. This same situation using SAML without the proposed extension, CSP2 and IdP1 will not interact, or they will require manual intervention from administrators to configure both ones.

CONCLUSION

A security enhanced and trust-aware IdM architecture compliance with SAMLv2/ID-FF standards is used to provide an efficient identity management and access control, as well as dynamic, autonomic, and user-centric system for better scalability in consumer cloud computing services. With the addition of reputation information and the introduction of the Trust-Aware ECP, mobile users may take part in the cloud federation in a more active way. Similarly, the presented reputation extensions allow the cloud providers to make richer trust decisions when interacting with unknown entities. In regard to privacy, the privacy enhanced and trust-aware IdM system allows users to access cloud services and share digital content without essentially revealing their true identity to everyone. Besides, security enhanced and trust-aware provides a framework that facilitates to keep to a trace-off between user's privacy and degree of tracking to obtain an enough personalization degree in the different services. Finally, privacy engine enables users to have enhanced awareness over their online identity use by introducing monitoring tools and an audit service focused on data sharing through the Personal Cloud.

In future the optimal values of parameters of reputation model can be validated.

REFERENCES

[1] Rosa Sanchez, Patrica Arias, "Enhancing Privacy and Dynamic Federation in Idm for Consumer Cloud Computing", IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, pp.95-103, February 2012.

[2] V. Krishna Reddy et.al, "Security Architecture Of Cloud Computing", International Journal Of Engineering Science and Technology, September 2011.

[3] Rafael Moreno- Vozmediano, Rubén S. Montero, and Ignacio M. Llorente Complutense University of Madrid "Key Challenges in Cloud Computing Enabling the Future Internet of Services" IEEE Computer Society, 2013.

[4] Jianyong Chen, Yang Wang, and Xiaomin Wang, Shenzhen University, China "On Demand Security Architecture for Cloud Computing", IEEE Research Feature ,2012.

[5] Rohit Ranchal, Bharat Bhagarva, "Protection of Identity Information in Cloud Computing without Trusted Third Party", IEEE International Symposium 2010.

[6] Bharat Bhargava1, Noopur Singh2, Asher Sinclair 3. "Privacy in Cloud Computing Through Identity Management " GIT Journal Of Engineering and Technology, 2011.

[7] Libor Sarga Faculty of Management and Economics Tomas Bata University in Zlin Czech Republic "Cloud Computing: An Overview", Journal Of Systems Integration, 2012.

[8] Ajey Singh, Dr. Maneesh Shrivastava "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[9] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, 2012.

[10] Hassan Takabi and James B.D. Gail-Joon Ahn Joshi "Security and Privacy Challenges in Cloud Computing Environments", IEEE Computer and Reliability Societies, 2012.

[11] Rajesh Piplode, Umesh Kumar Singh "An Overview and Study of Security Issues & Challenges in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 9, September 2012 .

[12] Anu Gopalakrishnan, “Cloud Computing Identity Management”, SETLabs Briefings Vol No. 7, 20.

[13] Rizwana Shaikh, M. Sasikumar “Identity Management in Cloud Computing “ International Journal of Computer Applications (0975 – 8887) Volume 63– No.11, February 2013.

[14] Marc Barichi, Elena Garcia2, Mario 3, “Security and Privacy Enablers for Future Identity Management Systems”, IEEE Transactions On Internet Security 2012.

[15] Archana N. Mahajan#, Sandip S. Patil ” Study and Review of Various Identity and Privacy Management Techniques in Consumer Cloud Computing”, GIT-Journal of Engineering and Technology (Sixth volume, 2013, ISSN 2249 – 6157).

[16] Meiko Jensen, J¨org Schwenk “On Technical Security Issues in Cloud Computing”, IEEE International Conference on Cloud Computing,2009.

[17] Alessandro Acquisti, “Identity M anagement, Privacy, and Price Discrimination”, IEEE Computer Society, 2008.

[18] Siani Pearson,“Taking Account of Privacy when Designing Cloud Computing Services”, Hewlett-Packard Development Company,2009.

[19] W. Chadwick and George Inman, “Attribute Aggrgation in Federated Identity Management”, IEEE Computer Society, May 2009.

[20] Federica Paci, Elisa Bertino, “Privacy-preserving Digital Identity Management for Cloud Computing”, IEEE Computer Society Technical Committee on Data Engineering, 2009.

[21] Leszek Lilien, Senior Member, IEEE, and Bharat Bhargava “A Scheme for Privacy-Preserving Data Dissemination”, IEEE Transactions on Systems, May 2009.

[22] Ramkinker Singh, Vipra Gupta, Mohan K. “Dynamic Federation in Identity Management for Securing and Sharing Personal Health Records in a Patient centric Model in Cloud”, International Journal of Engineering and Technology, June 2013.

[23] Pelin Angin, Bharat Bhargava, Rohit Ranchal, Noopur Singh “An Entity-centric Approach for Privacy and Identity Management in Cloud Computing”.

[24] Miska Laakkonen, “Identity federation and Identity Providers”.

[25] F. Almenárez, P. Arias, D. Diaz Sanchez, A. Marin, and R. Sanchez, “fed TV: Personal Networks Federation for Idm in Mobile DTV”, IEEE Transactions on Consumer Electronics, vol.57, no.2, May 2011.

[26] Matt Blaze, “Dynamic Trust Management”, IEEE Computer, Volume 42, Issue 2, February 2009, pages 44-52.

[27] Patricia Arias Cabarcos, Florina Almen´arez Mendoza, Andr´es Mar´ın-L´opez, and Daniel D´ıaz-S´anchez, “Enabling SAML for Dynamic Identity Federation Management”.

[28] John Steven,Gunnar Peterson, gunnar “Dynamic Security Assertion Markup Language Simplifying Single Sign-On”, IEEE Computer Society, 2007.

[29] Kelly D. LEWIS, James E. LEWIS, Ph.D, “Web Single Sign-On Authentication using SAML”, International Journal of Computer Science Issues, Vol. 2, 2009.

[30] Slawomir Grzonkowski and Peter M. Corcoran “Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking” IEEE Transactions on Consumer Electronics, Vol. 57, No. 3, August 2011.

[31] Li Lu, Member, IEEE, Jinsong Han, Member, IEEE, Yunhao Liu, Senior Member, IEEE, Lei Hu, Jinpeng Huai, Member, IEEE, Lionel M. Ni, Fellow, IEEE, and Jian Ma “Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps”, IEEE Transactions on Parallel and Distributed Systems, October 2008.

[32]Liladhar R. Rewatkar, Ujwal A. Lanjewar,”Implementation of Cloud Computing on Web” International Journal of Computer Applications, Volume 2 – No.8, June 2010.

[33] Sven Bugiel1, Stefan N • urnberger1, Ahmad-Reza Sadeghi1, Thomas Schneider “Twin Clouds: An Architecture for Secure Cloud Computing” ,2010.