Cloud Computing Security with Identity-Based Authentication Using Heritage-Based Technique

Rishi Kumar Sharma[1], Dr. R.K.Kapoor[2]

[1]Computer Science, AISECT University, Bhopal, India
[2]Computer Science, NITTTR, Bhopal, India

Abstract— *More organizations start to give various types of distributed computing administrations for Internet clients in the meantime these administrations additionally bring some security issues. Presently the many of cloud computing systems endow digital identity for clients to access their services, this will bring some drawback for a hybrid cloud that includes multiple private clouds and/or public clouds. Today most cloud computing framework use asymmetric and traditional public key cryptography to give information security and common authentication. Identity-based cryptography has some attraction attributes that appear to fit well the necessities of cloud computing. In this paper, by receiving federated identity management together with hierarchical identity-based cryptography (HIBC) with cloud heritage technique, not only the key distribution but also the mutual validation can be rearranged in the cloud.*

Keywords— cloud computing, cloud heritage, security, authentication.

I. INTRODUCTION

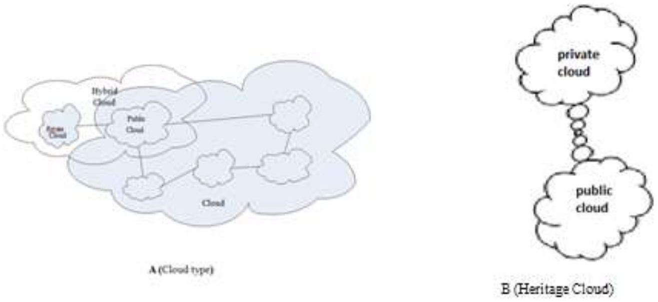
Cloud computing is a technique of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. It is the result of improvement of infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS).With broadband Internet access, Internet clients are able to occupy computing resource, storage space and different kinds of software services according to their necessities. In the cloud heritage, with a lot of different computing resources, client can easily tackle their issues with the resources gave by a cloud. This brings incredible adaptability for the clients. Using cloud computing service, clients can store their basic data in servers and can get their data anyplace they can with the Internet and do not have to stress about system breakdown or disk faults, etc. Also, distinctive clients in one system can share their data and work. Numerous important organizations, for example Amazon, Google, IBM, Microsoft, and Yahoo are the forerunners that give cloud computing services.

Cloud heritage is a concept of object oriented .The capability of one cloud to inherit services from another cloud is called cloud heritage. This is the property of client oriented network.

As of now, as appeared in Figure 1, there are essentially three sorts of clouds: private clouds, public clouds and hybrid clouds [15]. Private clouds, likewise called internal clouds, are the private networks that offer cloud computing services for a very restrictive set of clients within internal network. Public clouds or external clouds refer to clouds in the conventional sense [13] Hybrid clouds are the clouds that incorporate different private and/or public clouds [14]. Giving security in a private cloud and a public cloud is easier, comparing with a hybrid cloud since commonly a private cloud or a public cloud only has one service provider in the cloud. Giving security in a hybrid cloud that consisting multiple service providers is much more difficult especially for key distribution and mutual authentication, so we are use cloud heritage technique. Also for client to access the services in a cloud, a client digital identity is needed for the servers of the cloud to manage the access control. While in the entire cloud, there are numerous different types of clouds and each of them has its own identity management system. Thus client who needs to get services from various clouds needs numerous digital identities from various clouds, which will bring disservice for clients. Using federated identity management, every client will have his unique digital identity and with this identity, he can get various services from various clouds.

Identity-based cryptography [10] could be a public key technology that permits the shopper of a public symbol of as hopper because the client's public key. Hierarchy identity-based cryptography is that the improvement from it so asto resolve the measurability drawback. Recently identity-based cryptography and hierarchy identity-based cryptography are projected to supply security for a few web applications.

This paper proposes to use united identity management within the heritage cloud specified each shopper and each server can have its own distinctive identity. With this distinctive identity and graded identity-based cryptography (HIBC), the key distribution and mutual authentication will be greatly simplified.



A (Cloud type)

B (Heritage Cloud)

Fig. 1:

II. SECURITY IN CLOUD COMPUTING

Cloud computing have numerous advantages in cost diminishment, resource sharing, time saving for new service deployment. While in a cloud computing system, major part data and software that clients use reside on the Internet, which bring some new difficulties for the system, particularly security and privacy. Since every application may use resource from various servers. The servers are possibly based at multiple locations and the services provided by the cloud may use various infrastructures across organizations. All these attributes of cloud computing make it complicated to give security in cloud computing. To ensure adequate security in cloud computing, different security issues, for example, authentication, data confidentiality and integrity, and non-repudiation, all need to be contracted into account.

As such that before, there square measure 3 varieties of clouds in general: non-public cloud, public cloud and hybrid cloud. during a public cloud, resources square measure dynamically provisioned on a fine-grained, self-service basis over the net. Services within the cloud square measure provided by associate degree off-site third-party supplier WHO shares resources and bills on a fine-grained utility computing basis. whereas in most non-public clouds, with restricted computing resources, it's troublesome for a personal cloud to supply all services for his or her consumer, as some services could additional resources than internal cloud will offer. Cloud heritage technique could be a potential answer for this issue since they will get the computing resources from external cloud computing suppliers. non-public clouds have their blessings in corporation governance and provide reliable services, furthermore as they permit additional management than public clouds do. For the protection issues, once a cloud surroundings is formed within a firewall, it will offer its shoppers with less exposure to net security risks. conjointly within the non-public cloud, all the services may be accessed through internal connections instead of public net connections, that build it easier to use existing security measures and standards. this could build non-public clouds additional acceptable for services with sensitive information that has got to be protected. whereas during a hybrid cloud, it includes quite one domain, which can increase the issue of security provision, particularly key management and mutual authentication. The domains during a hybrid cloud may be heterogeneous networks, thus there could also be gaps between these networks and between the various services suppliers. Even security may be well secure in every of private/public cloud, whereas during a hybrid cloud with quite one reasonably clouds that have completely different| completely different} styles of network conditions and different security policies, the way to offer economical security protection is way harder.

In a cloud, the cloud ADPS must offer a robust and client-friendly method for purchasers to access every kind of services within the system. Once a consumer desires to run AN application within the cloud, the consumer is needed to produce a digital identity. Normally, this identity may be a set of bytes that associated with the consumer. Supported the digital identity, a cloud system will apprehend what right this consumer has and what the consumer is allowed to try and do within the system. Most of cloud platforms embrace AN identity service since identity data is needed for many distributed applications [3]. These cloud computing systems can offer a digital identity for each consumer.

To solve these problems in the cloud, we offer to use federated identity management in clouds with HIBC and CHT. The proposed scheme does not only allow clients from a cloud to access services from other clouds with a single digital identity, it also over-simplify the key distribution and mutual authentication in a heritage cloud.

III. IDENTITY-BASED CRYPTOGRAPHY AND SIGNATURE

Identity-based cryptography and signature schemes were foremost projected by Shamir [10] in 1984. however solely in 2001, a economical approach of identity-based encoding schemes was developed by Dan Boneh and Matthew K. Franklin [2] and Clifford Cocks [4]. These schemes ar supported additive pairings on elliptic curves and have obvious security. Recently stratified identity-based cryptography (HIBC) has been projected in [6, 7] to enhance the measurability of ancient identity-based cryptography theme.

Identity-based scientific discipline theme could be a reasonably public-key based mostly approach which will be used for 2 parties to exchange messages and effectively verify every other's signatures. in contrast to in ancient public-key systems that employing a random string because the public key, with identity-based cryptography shopper's identity which will unambiguously determine that client is employed because the public key for secret writing and signature verification. Identity-based cryptography will ease the key management quality as public keys don't seem to be needed to be distributed firmly to others. Another advantage of identity-based secret writing is that secret writing and coding are often conducted offline while not the key generation center.

In the identity-based cryptography approach, the PKG ought to creates a "master" public key and a corresponding "master" non-public key first off, then it'll create this "master" public key public for all the interested shoppers. Any shopper will use this "master" public key and also the identity of a shopper to make the general public key of this shopper. every shopper desires to urge his non-public key must contact the PKG together with his identity. PKG can use the identity and also the "master" non-public key to get the non-public key for this shopper. In Dan Boneh and Matthew K. Franklin's approach, they outlined four algorithms for a whole identity-based cryptography system. It includes setup, extract, secret writing and decipherment.

1. **Setup:** PKG create a master key K_m and the system parameters P. K_m is kept secret and used to generate private key for clients. System parameters P are made public for all the clients and can be used to generate clients' public key with their identities.
2. **Extract:** When a client requests his private key from the PKG, PKG will use the identity of this client, system parameters P and master key K_m to gener-ate a private key for this client.
3. **Encryption:** When a client wants to encrypt a message and send to another client, he can use the system parameters P, receiver's identity and the message as input to generate the cipher text.
4. **Decryption:** Receiving a cipher text, receiver can use the system parameters P and his private key got from the PKG to decrypt the cipher text.

In a network mistreatment identity-based cryptography, the PKG wants not solely to come up with personal keys for all the shoppers, however additionally to verify the shopper identities and establish secure channels to transmit personal keys. during a giant network with only 1 PKG, the PKG can have a onerous job. during this case, HIBC [6] will be a far better alternative. during a HIBC network, a root PKG can generate and distribute personal keys for domain-level PKGs and therefore the domain-level PKGs can generate and distribute personal keys to the shoppers in their own domain. HIBC is appropriate for an oversized scale network since it will scale back the work of root PKG by distribute the work of shopper authentication, personal key generation and distribution to the various level of PKGs. It can even improve the safety of the network as a result of shopper authentication and personal key distribution will be done regionally. The HIBC secret writing and signature algorithms embrace root setup, lower-level setup, extraction, encryption, and decipherment.

1. **Root setup:** root PKG will generate the root PKG system parameters and a root secret. The root secret will be used for private key generation for the lower-level PKGs. The root system parameters are made publicly available and will be used to generate public keys for lower-level PKGs and clients.
2. **Lower-level setup:** Each lower-level PKG will get the root system parameters and generate its own lower-level secret. This lower-level secret will be used to generate private keys for the clients in its domain.
3. **Extract:** When a client or PKG at level t with its identity ($ID_{1,...,} ID_t$) re-quests his private key from its upper-level PKG, where ($ID_{1,...,} ID_i$) is the identity of its ancestor at level i ($1 \leq i \leq t$), the upper-level PKG will use this identity, system parameters and its own private key to generate a private key for this client.
4. **Encryption:** Client who wants to encrypt a message M can use the system parameters, receiver's identity and the message as input to generate the cipher text.
   C = Encryption (parameters, receiver ID, M).
5. **Decryption:** Receiving a cipher text, receiver can use system parameters and his private key got from the PKG to decrypt the cipher text.
   M = Decryption (parameters, k, C), k is the private key of the receiver
6. **Signing and verification:** A client can use parameters, its private key, and message M to generate a digital signature and sends to the receiver. Receiver and verify the signature using the parameters, message M, and the sender's ID.
   Signature = Signing (parameters, k, M),
   k is the sender's private key.
   Verification = (parameters, sender ID, M,Signature).

There ar some inherent limitations with the identity-based cryptography [1]. one amongst downsides} is that the key written agreement problem. Since clients' non-public keys ar generated by PKG, the PKG will rewrite a client's message and build any client's digital signature while not authorization. This really implies that PKGs should be extremely trusty. that the identity-based theme is additional applicable for a closed cluster of shoppers like an enormous company or a university. Since solely beneath this example, PKGs will be established with clients' trust.

In a system exploitation HIBC, each PKG within the hierarchy is aware of the clients' non-public keys within the domain beneath the PKG. though key written agreement drawback cannot be avoided, this will limit the scope of key written agreement drawback. Another disadvantage of the identity-based cryptography is that the revocation drawback. as a result of all the purchasers within the system use some distinctive identifiers as their public keys, if one client's non-public key has been compromised, the shopper ought to modification its public key.

IV. USING FEDERATED IDENTITY MANAGEMENT IN CLOUD

4.1 Federated Identity Management in the Cloud

Compared with centralized identity, that is employed to take are of security issues among constant networks, federate identity is adopted to take care of the safety issues that a consumer might want to access external networks or associate degree external consumer might want to access internal networks. federate identity may be a standard-based mechanism totally different|for various} organization to share identity between them and it will change the movability of identity info to across different networks. One common use of federate identity is secure net single sign-on, wherever a consumer World Health Organization logs in with success at one organization will access all partner networks while not having to log in once more. mistreatment identity federation will increase the safety of network since it solely needs a consumer to spot and attest him to the system for just one occasion and this identity info are often utilized in totally different networks. Use of identity federation standards cannot solely facilitate the consumer to across multiple networks embrace external networks with just one time log in, however can also facilitate purchasers from totally different networks to trust one another.

Using identity federation within the cloud means that shoppers from totally different clouds will use a united identification to spot themselves, that naturally suit the necessity of identity based mostly cryptography in cloud computing. In our approach, server to server, shoppers and servers within the cloud have their own distinctive identities. These identities area unit class-conscious identities. To access services within the cloud, shoppers area unit needed to attest themselves for every service in their own clouds. In some cases, servers also are needed to attest themselves to shoppers. in an exceedingly little and closed cloud, this demand will be happy simply. whereas in an exceedingly hybrid cloud, there area unit multiple non-public and/or public clouds and these clouds could have faith in totally different authentication mechanisms. Providing effective authentications for shoppers and servers from totally different cloud domains would be tough. during this paper, we have a tendency to propose to use united identity management and HIBC with cloud heritage technique within the cloud. within the cloud trustworthy authority PKGs area unit used and these PKGs won't solely act as PKGs in ancient identity-based cryptography system however conjointly apportion class-conscious identities to shoppers in their domains. there's a root PKG in overall domain of every cloud, and every sub-level domain (private or public cloud) inside the cloud heritage conjointly has its own PKG. the basis PKG can manage the full heritage cloud, every non-public cloud or public cloud is that the 1st level and shoppers and servers in these clouds area unit the second level. the basis PKG of the cloud can apportion and attest identities for all the non-public and public clouds.

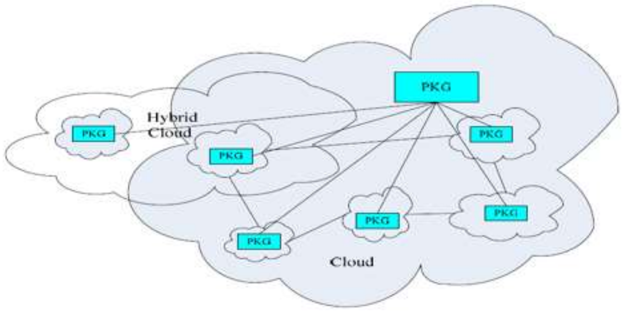


Fig.2: Federated identity management in cloud

4.2: Key Generation and in the Cloud

Using HIBC in the heritage cloud, an important part is key generation and distribution. As shown in [6], the security of HIBC scheme is based on the using of admissible pairing. Let G_1 and G_2 be two groups of some large prime order q and $_{G\ 1}$ is an additive group and 2 G is a multiplicative group, we can call ˆe an admissible pairing if ˆ e :

$G\ 1 \times G\ 2 \rightarrow G\ 2$ have the following properties.

1. **Billinear:** For all 1 P , $Q \in G$ and , $q\ a\ b \in Z*$, $e\hat{}(aP, bQ) = e\hat{}(P,Q)ab$.

2. **Non-degenerate:** There exits 1 $P,Q \in G$, such that $e\hat{}(P,Q) \neq 1$.

3. **Computable:** For all 1 $P,Q \in G$, there exits a efficient way to calculate

$e\hat{}(P ,Q)$.

An admissible pairing can be generated by suing a Weil pairing or a Tate pairing [2]. Here, in the cloud we use two levels PKG, the root PKG is 0 *level* PKG and the

PKGs in the private or public clouds are 1 *level* PKGs. The root setup can be done as follow:

1. Root PKG generates G_1 , G_2 and an admissible pairing $\hat{e}(aP,bQ)=\hat{e}(P,Q) \neq 1(G_1,G_2,\hat{e},P_0,Q_0,H_1,H_2)$ $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$.
2. Root PKG chooses $P_0 \in G_1$ and $s_0 \in Z_q^*$ and set $Q_0 = s_0P_0$.
3. Root PKG chooses hash function $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : G_2 \rightarrow \{0,1\}^*$.

Then the system parameters are $(G_1,G_2,\hat{e},P_0,Q_0,H_1,H_2)$ and are public available. s_0 is the root PKG's secret and is known only by the root PKG.

For the lower level PKGs and users and servers in the cloud, they can use the system parameters and any user's identity to generate its public key. And every user or servers in the cloud can connect the PKGs in their cloud domain to get their private keys. For example, the PKG in private cloud of University with identity UIS, its public key can be generated as

$P_{uis} = H_1(UIS)$ and the root PKG can generate its private key as $s_{uis} = s_0P_{uis}$. For a user with identity UIS.Alice in the private cloud University of Stavanger , her public key can be generated as $P_{uisalice} = H_1(UIS \| Alice)$ and the PKG can generate her private key as $s_{uisalice} = s_{uis} + s_{uis}P_{uisalice}$.

4.3 Date Encryption and Digital Signature

In the cloud, one amongst the foremost necessary security issues ar mutual authentication between shoppers and servers, protection knowledge|of knowledge|of information} confidentiality and integrity throughout data transmission by secret writing victimisation secret keys. in a very cloud victimisation united identity, any shopper and server has its distinctive identity and any shopper and server will get the identity of the other client/server by request with the PKGs. With HIBC, the general public key distribution are often greatly simplified within the cloud. shoppers and servers don't have to be compelled to raise a public key directory to induce the general public key of alternative shoppers and servers as in ancient public key schemes. If any shopper or server desires to encipher the info that transmitted within the cloud, the sender will acquire the identity of the receiver, then the sender will en-crypt the info with receiver's identity.

4.4 Secret Session Key Exchange and Mutual Authentication

Identity-based cryptography is a public key cryptography scheme, it is much slower when it is compared with symmetric key cryptography. In practice, public key cryptography is not used for data encryption in most of the clouds. While in the cloud with HIBC, this secret symmetric key distribution can be avoided since identity-based cryptography can be used for secret session key exchange. According to [9], for every two parties in the system using identity-based cryptography, it is easy for each one of the two parties to calculate a secret session key between them using its own private key and public key of other party, this is call identity-based non-interactive key distribution. For example, two parties Alice and Bob in a cloud with their public keys and private keys P_{alice} , Q_{alice} , P_{bob} and Q_{bob} can calculate their shared secret session key by computing

$$K_s = \hat{e}(Q_{alice}, P_{bob}) = \hat{e}(Q_{bob}, P_{alice}) \qquad (1)$$

This means in an exceedingly cloud victimization HIBC, every shopper or server will calculate a secret session key between it and therefore the different party it needs to speak with while not message exchange. This advantage of identity-based cryptography can't solely scale back mes-sage transmission however can also avoid session key revelation throughout transmission.

This secret session key can be used not only for data encryption, but also for mu-tual authentication [8]. We assume if a client with identity *Alice@UiS* and a server with identity *Storage@google* in the cloud want to authenticate each other. First, they can calculate a secret session key K_s between them. Then Alice can send a message to the server as:

$$Alice \rightarrow Server : Alice@UiS, M, f(K_s, Alice@UiS, Storage@google, M)$$

Here *M* is a randomly selected message and *f* is a one way hash function. Here, to compute the correct hash value, a correct secret session key K_s is needed. Since K_s computation requires Alice's private key and this private key can only be allocated from the PKG in the private cloud, thus Alice can be verified that she is a legal client of this cloud. Also the server can authenticate itself to Alice the same way. We can notice that this mutual authentication does not include any certification form a third party.

4.5 Key Escrow

For a system exploitation identity-based cryptography, key written agreement downside is inherent and may not be avoided since PKG is aware of the non-public keys of all the shoppers. whereas within the ranked identity-based cryptography system, solely the PKG within the same domain because the shoppers will is aware of their non-public keys. PKGs in different domains or at different levels cannot apprehend these non-public keys, such the key written agreement downside may be restricted in an exceedingly little vary.

V. CONCLUSION

The quick development of cloud computing bring some security issues similarly as several edges to net purchasers. Current solutions have some disadvantages in key management and authentication particularly in a very hybrid cloud with many public/private clouds. during this paper, we have a tendency to portrayed the principles of identity-based cryptography heritage technique and gradable identity-based cryptography and notice the properties of HIBC match well with the protection demands of heritage cloud. we have a tendency to projected to use federate identity management and HIBC within the cloud and portrayed however will the system generate and distribute the general public and personal keys to purchasers and servers. Compared with the present Ws-Security approach, we will see our approach has its blessings in simplifying public key distribution and reducing SOAP header size. additionally we have a tendency to showed however the purchasers and servers within the cloud will generate secret session key while not message exchange and demonstrate one another with an easy manner mistreatment identity-based cryptography. additionally we will see the key written agreement downside of identity-based cryptography are often restricted with HIBC approach.

REFERENCES

[1] Beak, J., Newmarch, J., Safavi-Naini, R., Susilo, W.: A Survey of Identity-Based Cryptography.

[2] In: Proc. of the 10th Annual Conference for Australian Unix User's Group (AUUG2004), pp. 95–102 (2004)

[3] Boneh, D., Franklin, M.: Identity-based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 433–439. Springer, Heidelberg (2001)

[4] Chappell, D.: A Short Introduction to Cloud Platforms, http://www.davidchappell.com/CloudPlatforms–Chappell.pdf

[5] Cocks, C.: An Identity-based Encryption Scheme Based on Quadratic Residues. In: Proceeding of 8th IMA International Conference on Cryptography and Coding (2001)

[6] Crampton, J., Lim, H.W., Paterson, K.G.: What Can Identity-Based Cryptography Offer to Web Services? In: Proceedings of the 5th ACM Workshop on Secure Web Services (SWS 2007), Alexandria, Virginia, USA, pp. 26–36. ACM Press, New York (2007)

[7] Gentry, C., Silverberg, A.: Hierarchical ID-Based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002)

[8] Horwitz, J., Lynn, B.: Toward Hierarchical Identity-Based Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (2002)

[9] Mao, W.: An Identity-based Non-interactive Authentication Framework for Computational Grids. HP Lab, Technical Report HPL-2004-96 (June 2004)

[10] Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Proceedings of the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan (January 2000)

[11] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)

[12] Lim, H.W., Robshaw, M.J.B.: On identity-based cryptography and GRID computing. In: Bubak, M., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2004. LNCS, vol. 3036, pp. 474–477. Springer, Heidelberg (2004)

[13] Lim, H.W., Paterson, K.G.: Identity-Based Cryptography for Grid Security. In: Proceedings of the 1st IEEE International Conference on e-Science and Grid Computing (e- Science 2005). IEEE Computer Society Press, Los Alamitos (2005) Defining Cloud Services and Cloud Computing, http://blogs.idc.com/ie/?p=190

[14] IBM Embraces Juniper For Its Smart Hybrid Cloud, Disses Cisco (IBM), http://www.businessinsider.com/2009/2/ibm-embraces-juniper-for-its-smart-hybrid-cloud-disses-cisco-ibm

[15] http://en.wikipedia.org/wiki/Cloud_computing#cite_note-61

[16] XML Signature Syntax and Processing (Second Edition) ,http://www.w3.org/TR/xmldsig-core/#sec-KeyInfo

[17] Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–368. Springer, Heidelberg (2002)

[18] M. Turner, D. Budgen, and P. Brereton, "Turning software into a service," Computer, vol. 36, no. 10, pp. 38–44, 2003.

[19] T. Oreilly, "What is Web 2.0: Design patterns and business models for the next generation of software," O'Reilly Media, Tech. Rep., 2008. [Online]. Available: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

[20] R. Buyya, C. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in

Conference on High Performance Computing and Communications. IEEE, 2008.

[21] A. Newman, A. Steinberg, and J. Thomas, Enterprise 2.0 Implementation.McGraw-Hill Osborne Media, 2008.

[22] Amazon, “Amazon Elastic Compute Cloud (EC2),” Amazon Web Services LLC, Tech. Rep., 2009. [Online]. Available: http://aws.amazon.com/ec2/

[23] Mosso, “Deploy and scale websites, servers and storage in minutes,” Rackspace, Tech. Rep., 2009. [Online]. Available: http://www.mosso.com/

[24] R. Buyya, C. Yeo, and S. Venugopal, “Market-oriented Cloud Computing: Vision, hype, and reality for delivering it services as computing utilities,” in High Performance Computing and Communications. IEEE Press, 2008.

[25] Google, “Google App Engine: Run your web apps on Google’s infrastructure.” Google, Tech. Rep., 2009. [Online]. Available:http://code.google.com/appengine/

[26] T. Bain, “Is the relational database doomed?” ReadWriteWeb.com, 2008. [Online]. Available: http://www.readwriteweb.com/archives/is the relational database doomed.php

[27] F. Chang, J. Dean, S. Ghemawat, W. Hsieh, D. Wallach, M. Burrows, T. Chandra, A. Fikes, and R. Gruber, “Bigtable: A distributed storage system for structured data,” in USENIX Symposium on Operating Systems Design and Implementation, 2006.

[28] G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, Pilchin, S. Sivasubramanian, P. Vosshall, and W. Vogels, “Dynamo: Amazon’s highly available key-value store,” in Symposium on Operating Systems Principles. ACM, 2007, pp. 205–220.

[29] B. Johnson, “Cloud Computing is a trap, warns GNU founder Richard Stallman,” The Guardian, Tech. Rep., 2008. [Online]. Available: http://www.guardian.co.uk/technology/2008/sep/29/ cloud.computing.richard.stallman

[30] J. McCabe, Network analysis, architecture, and design. Morgan Kaufmann, 2007. [Online]. Available: http://books.google.co.uk/books?id=iddGPgR48 MC

[31] A. Modine, “Web startups crumble under Amazon S3 outage,” The Register, Tech. Rep., 2008. [Online]. Available: http://www.theregister.co.uk/2008/02/15/amazon s3 outage feb 2008/

[32] J. Montgomery, “Google Apps sees 99.9reliability”,” Tech.Blorge, Tech. Rep., 2008. [Online]. Available: http://tech.blorge.com/Structure:%20/2008/11/ 02/google-apps-sees-999-uptime-proves-cloud-reliability/

[33] J. Perez, “Google Apps customers miffed over downtime,”IDG News Service, Tech. Rep., 2007. [Online].Available: http://www.pcworld.com/businesscenter/article/ 130234/google apps customers miffed over downtime.html

[34] Kable, “Carter recommends ’g cloud’ for gov it,” The Register,2009. [Online]. Available: http://www.channelregister.co.uk/2009/06/17/gover nment cloud computing/

[35] Environmental Protection Agency, “EPA report to congress on server and data center energy efficiency,” US Congress, Tech.Rep., 2007.

[36] R. Miller, “NSA maxes out Baltimore power grid,” Data Center Knowledge, Tech. Rep., 2006. [Online]. Available: http://www.datacenterknowledge.com/archives/2006/ 08/06/nsa-maxes-out-baltimore-power-grid/

[37] K. McIsaac, “The data centre goes green, the CFO saves money,” Intelligent Business Research Services, Tech. Rep., 2007.

[38] C. Wolf and E. Halter, Virtualization: from the desktop to the enterprise. Apress, 2005.

[39] R. Talaber, T. Brey, and L. Lamers, “Using virtualization to improve data center efficiency,” The Green Grid, Tech. Rep., 2009.

[40] K. Brill, “The invisible crisis in the data center: The economic meltdown of Moore’s law,” Uptime Institute, Tech. Rep., 2007.

[41] J. Brodkin, “Gartner in ‘green’ data centre warning,” Techworld, 2008. [Online]. Available: http://www.techworld.com/green-it/news/index.cfm?newsid=106292

[42] Microsoft, “Azure services platform,” Micrsoft, Tech. Rep., 2009.[Online]. Available: http://www.microsoft.com/azure/

[43] C. Metz, “The Meta Cloud - flying data centers enter fourth dimension,” The Register, Tech. Rep., 2009. [Online]. Available: http://www.theregister.co.uk/2009/02/24/the meta cloud/

[44] T. Kulmala, “The cloud’s hidden lock-in: Latency,” Archivd, 2009. [Online]. Available: http://blog.archivd.com/1/post/2009/04/the-clouds-hidden-lock-in-latency.html

[45] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, “The Eucalyptus open-source cloud-computing system,” in Cloud Computing and Its Applications, 2008.

[46] J. Abbate, Inventing the internet. MIT press, 1999.

[47] I. Foster and C. Kesselman, The grid: blueprint for a new computing infrastructure. Morgan Kaufmann, 2004.

[48] G. Briscoe and P. De Wilde, “Digital Ecosystems: Evolving service-oriented architectures,” in Conference on Bio Inspired Models of Network, Information and Computing Systems. IEEE Press, 2006. [Online]. Available: http://arxiv.org/abs/0712.4102

[49] G. Briscoe, “Digital ecosystems,” Ph.D. dissertation, Imperial College London, 2009.

[50] L. Rivera Le´on. Regions for Digital Ecosystems Network (REDEN). [Online]. Available: http://reden.opaals.org.