ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Improved Security, Energy Efficient Load Balancing for the Stable and Reliable Cloud

Mr. B. Subramani[1], Ms. B. Rajalakshmi[2]

HOD/Asst Professor, Dept of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore[1]

Research Scholar, Dept of Computer Science, Dr.N.G.P. Arts and Science College, Coimbatore[2]

Abstract: Cloud computing is a freshly industrializing new technology for multipart systems with large-level services distribution among various users. Therefore, verifying and validating of both users and services is a important issue for the confidence and protection of the cloud computing. SSL Authentication Protocol, once implemented in cloud computing, will become so complex that users will experience high overloaded issues in both calculation and communication. The proposed research is, based on the Attribute-based hierarchical method for cloud computing and its equivalent cryptographic and signature methods, presented a new Attribute-based security protocol for cloud computing and services. Through simulation testing, it is shown that the security protocol is more significant and capable than SSL Authentication Protocol, specially the more significant on user side.

Keywords: Cloud computing, Security, Attribute, Simulation, Protocol.

I. ABOUT CLOUD

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). Clouds can be classified as public, private or hybrid.
Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rackspace, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.
The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as one uses it). Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure.

Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Cloud vendors are experiencing growth rates of 50% per annum

II. INTRODUCTION

As more and more organizations adopt electronic records , the case for cloud data storage be- comes compelling for deploying ER systems: not only is it inexpensive but it also provides the exible, wide-area mobile access increasingly needed in the modern world. However, before cloud-based ER systems can become a reality, issues of data security, patient privacy, and overall performance must be addressed. As standard encryption (including symmetric key and public-key) techniques for ER encryption/decryption cause increased access control and performance overhead, the paper proposes the use of Attribute-Based Encryption to encrypt ERs based on providers' attributes or credentials; to decrypt ERs, they must possess the set of attributes needed for proper access.

This paper motivates and presents the design and usage of a ATTRIBUTE based ER system based on ABE, along with preliminary experiments and analyses to investigate the exibility and scalability of the proposed approach.

DOI 10.17148/IJARCCE.2015.4912

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

III. RELATED WORK

CHISTAR adopts the Cloud Component Model approach for application design described in our previous work. Cloud component model allows identifying the building blocks of a cloud application which are classified based on the functions performed and type of cloud resources required. Each building block performs a set of actions to produce the desired outputs for other components.

Less Scalability: Cloud-based EHRs such as CHISTAR have better scalability as compared to client-server EHRs. CHISTAR adopts the Cloud Component Model approach for application design which provides better scalability by decoupling application components and providing asynchronous communication mechanisms. Since components are designed to process requests asynchronously, it is possible to parallelize the processing of requests. Using Cloud Component Model, CHISTAR can leverage both horizontal and vertical scaling options.

Less Maintainability: CHISTAR has better maintainability as compared to client-server based EHR systems. The functionality of individual components of CHISTAR can be improved or upgraded independent of other components. Loose coupling allows replacing or upgrading components, without changing other components. Since CHISTAR has loosely coupled components, it is more resilientto component failures. In case of client-server based EHR systems with tightly coupled components, failure of a single component can bring down the entire application.

Less Portability: Cloud-based EHR systems such as CHISTAR have better portability. By designing loosely coupled components that communicate asynchronously, it is possible to have innovative hybrid deployments in which different components of an application can be deployed on cloudinfrastructure and platforms of different cloud vendors.

Less Reduced Costs: Client-server EHR systems with dedicated hosting require a team of IT expertsto install, configure, test, run, secure and update hardware and software. With cloud-based HER systems, organizations can save on the upfront capital investments for setting up the computinginfrastructure as well as the costs of managing the infrastructure as all of that is done by the cloudprovider. Though hardware maintenance overhead.

IV. MOTIVATION

In this section, we describe the motivation for an Attribute based ERs.

i. Design Methodologies

Using HIBC in the cloud, an important part is key generation and distribution. As the security of HIBC scheme is based on the using of admissible pairing.
Let 1 G and 2 G be two groups of some large prime order q and 1 G is an additive group and 2 G is a multiplicative group, we can call ˆe an admissible pairing if ˆ e : G 1 × G 2 → G 2 have the following properties.

1. **Bilinear:** For all 1 P , Q ∈ G and , q a b ∈ Z ∗ , eˆ(aP, bQ) = eˆ(P,Q)ab.
2. **Non-degenerate:** There exits 1 P,Q∈ G , such that eˆ(P,Q) ≠ 1.
3. **Computable:** For all 1 P,Q∈ G , there exitsa efficient way to calculate eˆ(P ,Q) .

An admissible pairing can be generated by suing a Weil pairing or a Tate pairing. Here, in the cloud we use two levels PKG, the root PKG is 0 levelPKG and the PKGs in the private or public clouds are 1 level PKGs. The root setup can be done as follow:

ii. Date Encryption and Digital Signature

In the cloud, one of the most important security problems are mutual authentication between users and servers, protection of data confidentiality and integrity during data transmission by encryption using secret keys. In a cloud using federated Attribute, any user and server has its unique Attribute and any user and server can get the Attribute of any other user/server by request with the PKGs. With HIBC, the public key distribution can be greatly simplified in the cloud. Users and servers do not need to ask a public key directory to get the public key of other users and servers as in traditional public key schemes. If any user or server wants to encrypt the data that transmitted in the cloud, the sender can acquire the Attribute of the receiver, and then the sender can encrypt the data with receiver's Attribute.

Currently, WS-Security (Web service Security) protocol which can provide end-to-end message level security using SOAP messages is widely applied in cloud computing to protect the security of most cloud computing related web services. WS-Security uses SOAP header element to carry security-related information. Since SOAP messageis a kind of XML message and ordinarily XML message representation is about 4 to 10 times large compared with their equivalent binary formats, adding security information into SOAP header will greatly increase the costs of data communication and data parsing.

iii. Secret Session Key Exchange and Mutual Authentication

Attribute-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. For example, in XML encryption, XML data is encrypted using symmetric cryptography such as AES andTriple-DES. This secret symmetric key is encrypted using the public key encryption and added in the SOAP message and then transmitted to the receiver. While in the cloud with HIBC, this secret symmetric key distribution can be avoided since Attribute- based cryptography can be used for secret session key exchange. According to for every two parties in the system using Attribute-based

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

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 Attribute-based non interactive key distribution. For example, two parties Alice and Bob in a cloud with their public keys and private keys alice P, alice Q , bob P and bob Q can calculate their shared secret session key by computing

$$K = e\ Q\ P = e\ Q\ P \quad (1)$$

This means in a cloud using HIBC, each user or server can calculate a secret session key between it and the other party it wants to communicate with without message exchange. This advantage of Attribute-based cryptography can not only reduce message transmission but also can avoid session key disclosure during transmission. This secret session key can be used not only for data encryption, but also for mutual authentication. We assume if a user with AttributeAlice@UiSand a server with AttributeStorage@googlein the cloud want to authenticate each other. First, they can calculate a secret session key s K between them. Then Alice can send a message to the server as:: @ , , (, @ , @ ,) s Alice → Server A lice UiS M f K A lice UiSStorage go og le M Here M is a randomly selected message and f is a one way hash function.

iv. Using MA-ABE in the Public Domain

For the PUDs, our framework delegates the key management functions to multiple attribute authorities. In order to achieve stronger privacy guarantee for data owners, the Chase-Chow (CC) MA-ABE scheme is used, where each authority governs a disjoint set of attributes distributive. It is natural to associate the cipher text of a PFR document with an owner-specified access policy for users from PUD. However, one technical challenge is that CC MA-ABE is essentially a KP-ABE scheme, where the access policies are enforced in users' secret keys, and those key-policies do not directly translate to document access policies from the owners' points of view. By our design, we show that by agreeing upon the formats of the key-policies and the rules of specifying which attributes are required in the cipher text, the CC MA-ABE can actually support owner-specified document access policies with some degree of flexibility

V. PROPOSED ATTRIBUTE BASED EHR SYSTEM

Attribute-based cryptography and signature schemes were firstly proposed by Shamir but, a efficient approach of Attribute-based encryption schemes was developed by Dan Boneh and Matthew K. Franklin and Clifford Cocks. These schemes are based on bilinear pairings on elliptic curves and have provable security. Recently hierarchical Attribute-based cryptography (HIBC) has been proposed to improve the scalability of traditional Attribute-based cryptography scheme. In Fig.1 Attribute-based cryptographic scheme is a kind of public-key based approach that can be used for two parties to exchange messages and effectively verify each other's signatures. Unlike in traditional public-key systems that using a random string as the public key, with Attribute-based cryptography user's Attribute that can uniquely identify that user is used as the public key for encryption and signature verification. Attribute-basedcryptography can ease the key management complexity as public keys are not required to be distributed securely to others. Another advantage of Attribute-based encryption is that encryption and decryption can be conducted offline without the key generation center.

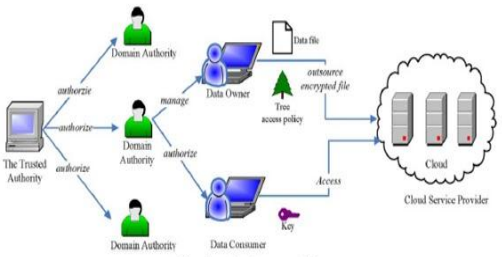


Fig. 1. System model.

In the Attribute-based cryptography approach, the PKG should creates a "master" public key and a corresponding "master" private key firstly, then it will make this "master" public key public for all the interested users. Any user can use this "master" public key and the Attribute of a user to create the public key of this user. Each user wants to get his private key needs to contact the PKG with his Attribute. PKG will use the Attribute and the "master" private key to generate the private key for this user. In Dan Boneh and Matthew K. Franklin's approach, they defined four algorithms for a complete Attribute-based cryptography system. It includes setup, extract, encryption and decryption.

1. **Setup:** PKG create a master key m K and the system parameters P. m K is kept secret and used to generate private key for users. System parameters P are made public for all the users and can be used to generate users' public key with their identities.

2. **Extract:** When a user requests his private key from the PKG, PKG will use the Attribute of this user, system parameters P and master key m K to generate a private key for this user.

3. **Encryption:** When a user wants to encrypt a message and send to another user, he can use the system parameters P, receiver's Attribute 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 using Attribute-based cryptography, the PKG needs not only to generateprivate keys for all the users, but also to verify the user identities and establish secure channels to transmit private keys. In a large network with only one PKG, the PKG will have a burdensome job. In this case, HIBC can be a better choice. In a HIBC network, a root PKG will

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

generate and distribute private keys for domain-level PKGs and the domain-level PKGs will generate and distribute private keys to the users in their own domain. HIBC is suitable for a large scale network since it can reduce the workload of root PKG by distribute the work of user authentication, private key generation and distribution to the different level of PKGs. It can also improve the security of the network because user authentication and private key distribution can be done locally. The HIBC encryption and signature algorithms include root setup, lower-level setup, extraction, encryption, and decryption.

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 availableand will be used to generate public keys for lower-level PKGs and users.

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 users in its domain.

Extract: When a user or PKG at level t with its Attribute(1,..., t ID ID) requests his private key from its upper-level PKG, where (1,..., i ID ID) is the Attribute of its ancestor at level i ($1 \leq i \leq t$), the upper-level PKG will use this172 L. Yan, C. Rong, and G. Zhao Attribute, system parameters and its own private key to generate a private keyfor this user.

Encryption: User who wants to encrypt a message M can use the system parameters, receiver's Attribute and the message as input to generate the cipher text. C = Encryption (parameters, receiver ID, M).

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.

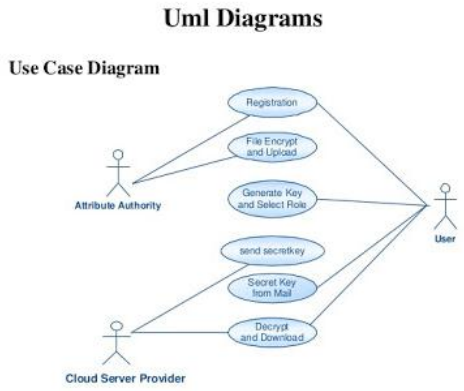


Fig.2 UML Diagram

Signing and verification: A user 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 are some inherent limitations with the Attribute-based cryptography. One of the issues is the key escrow problem. Since users' private keys are generated by PKG, the PKG can decrypt a user's message and create any user's digital signature without authorization. This in fact means that PKGs must be highly trusted. So the Attribute-based scheme is more appropriate for a closed group of users such as a big company or a university. Since only under this situation, PKGs can be set up with users' trust. In a system using HIBC, every PKG in the hierarchy knows the users' private keys in the domain under the PKG. Although key escrow problem can not be avoided, this can limit the scope of key escrow problem. Another drawback of the Attribute-based cryptography is the revocation problem. Because all the users in the system use some unique identifiers as their public keys, if one user's private key has been compromised, the user need to change its public key. For example, if the public key is theuser's name, address, or email address, it is inconvenient for the user to change it. One solution for this problem is to add a time period to the identifier as the public key, but it cannot solve this problem completely.

VI. BENEFITS

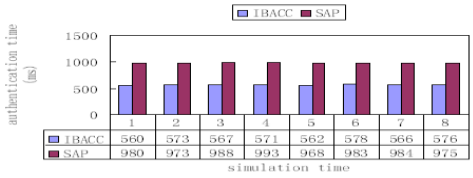
Cloud computing is the delivery of computing and storage capacity as a service to a community of end-recipients. With the development and application of cloud computing, its security becomes more and more important. In this paper, we gave a review on secure cloud storages, sub-offering within IaaS of cloud computing, which are designed by using cryptographic techniques. We focused on what type of cryptographic techniques is applied in the design of cloud storage and how to apply, not paid too much attention on the concrete design of these cloud storages. In the future, it is believed that more cryptographic techniques can be applied to cloud computing and more secure cloud storage systems can be proposed.

The platform of simulation experiment is Cloud Sim which is a simulation platform based on Java. Special users and resources can be generated by rewriting these interfaces. This aligns well with various users and resources of cloudcomputing. Furthermore, CloudSim is based on SimJava which is a discrete event simulation tool based on Java and simulates various entities by multiple threads. This aligns well with randomness of cloud computing entity action. Therefore, it is feasible to simulate our proposed authentication protocol of cloud computing by CloudSim.
The simulation environment is composed of four computers which are all equipped with P4 3.0 CPU, 2G memory. Certification chain is important for SAP. The shorter, the better. The shortest certification chain includes all 4 certifications: 1 CA, client and 2 CA, server. There

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

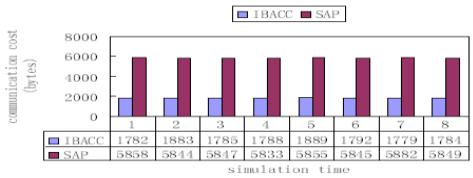
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

are a cross authentication for 1 CA and 2 CA. It is in this scene that SAP and IBACC are compared. Based on openssl0.9.7, SAP is implemented. Pairing computing adapts the algorithms of reference.To precisely simulate the network delay, there are 25~45ms waiting time beforemessages are sent.



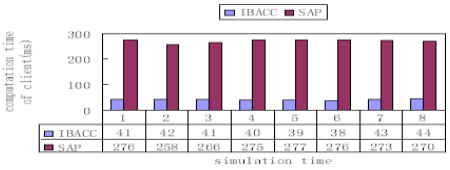
	1	2	3	4	5	6	7	8
IBACC	560	573	567	571	562	578	566	576
SAP	980	973	988	993	968	983	984	975

Fig. 3. Comparison of authentication time



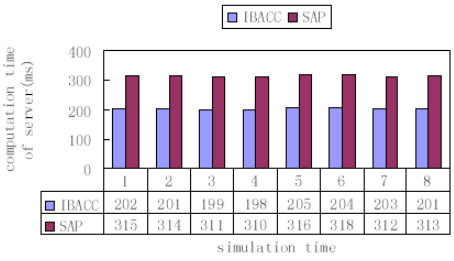
	1	2	3	4	5	6	7	8
IBACC	1782	1883	1785	1788	1889	1792	1779	1784
SAP	5858	5844	5847	5833	5855	5845	5882	5849

Fig. 4. Comparison of communication cost



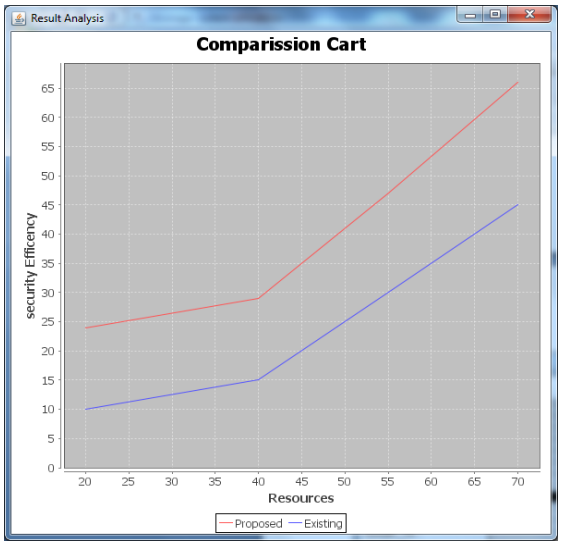
	1	2	3	4	5	6	7	8
IBACC	41	42	41	40	39	38	43	44
SAP	276	258	266	275	277	276	273	270

Fig. 5. Comparison of computation time of client



	1	2	3	4	5	6	7	8
IBACC	202	201	199	198	205	204	203	201
SAP	315	314	311	310	316	318	312	313

Fig. 6. Comparison of computation time of server



As shown in Fig.5, computation time of client for IBACC is approximately 41 ms while that for SAP is 272 ms. That is to say, computation time of client for IBACC is 15% of that for SAP. Fig.6 illustrates computation time of server for IBACC is approximately 202 ms while that for SAP is 313 ms. That is to say, computation time of server for IBACC is 65% of that for SAP.

The simulation results confirm that both client and server of IBACC are more lightweight than those of SAP. Furthermore, computation time of client is 20% of that of server in IBACC. This aligns well with the idea of cloud computing which allows the user with an average or low-end platform to outsource its computational tasks to more powerful servers. As a result, the more lightweight user side can connect more servers and contribute to the larger scalability.

VII. CONCLUSION& FUTURE WORK

Authentication is necessary in Cloud Computing. SSL Authentication Protocol is of low efficiency for Cloud services and users. In this paper, we presented an Attribute-based authentication for cloud computing, based on the Attribute-based hierarchical model for cloud computing and corresponding encryption and signature schemes. Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the authentication protocol is more efficient and lightweight than SSL Authentication Protocol, especially the more lightweight user side. This aligned well with the idea of cloud computing to allow the users with an average or low-end platform to outsource their computational tasks to more powerful servers.

The quick development of cloud computing bring some security problems as well as many benefits to Internet users. Current solutions have some disadvantages in key management and authentication especially in a hybrid cloud with several public/private clouds. In this paper, we depicted the principles of Attribute-based cryptography and hierarchical Attribute-based cryptography and find the properties of HIBC fit well with the security demands of cloud.

We have discussed how to provide data security by the client by using a method “digital signature” with auto-generated token which can make the world of cloud computing becomes more secure, reliable and admirable. The major benefit of using cloud computing is to reduce both capital expenditure on infrastructure as well as operational expenditure on infrastructure maintenance. From a data security perspective, it is possible to limit access to plain data by using trustworthy client.

In future this work can also be extended by providing encryption and decryption algorithms on digital signatures as well as on token number. In this way security becomes tighter. A major challenge towards cloud computing is to implementing the high traffic flow design by using different protocols. And some other challenges are Manageability, monitoring, availability, data governance, and reliability and virtualization security space.

DOI 10.17148/IJARCCE.2015.4912

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

REFERENCES

[1].Beak, J., Newmarch, J., Safavi-Naini, R., Susilo, W.: A Survey of Attribute-Based Cryptography. In: Proc. of the 10th Annual Conference for Australian Unix User's Group (AUUG 2004), pp. 95–102 (2004)

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

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

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

[5]. Crampton, J., Lim, H.W., Paterson, K.G.: What Can Attribute-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)

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

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

[8]. Dai, Y.S., Levitin, G.: Reliability and Performance of Tree-structured Grid Services. IEEE Transactions on Reliability 55(2), 337–349 (2006)

[9]. Dai, Y.S., Xie, M., Wang, X.L.: Heuristic Algorithm for Reliability Modeling and Analysis of Grid Systems. IEEE Transactions on Systems, Man, and Cybernetics, Part A 37(2), 189–200 (2007)

[10]. Boneh, D., Gentry, C., Hamburg, M.: Space Efficient Attribute Based Encryption without Pairings. In: Proceedings of FOCS 2007, pp. 647–657 (2007)

[11]. Boneh, D.: Generalized Attribute Based and Broadcast Encryption Schemes. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. Springer, Heidelberg (2008)

[12]. Boyen, X.: General Ad Hoc Encryption from Exponent Inversion IBE. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 394–411. Springer, Heidelberg (2007)

[13]. Lim, H.W., Robshaw, M.: On Attribute- 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)

[14]. Lim, H.W., Robshaw, M.: A dynamic key infrastructure for GRID. In: Sloot, P.M.A., Hoekstra, A.G., Priol, T., Reinefeld, A., Bubak, M. (eds.) EGC 2005. LNCS, vol. 3470, pp. 255–264. Springer, Heidelberg (2005)

[15]. Chen, L., Lim, H.W., Mao, W.B.: User-friendly grid security architecture and protocols. In: Proceedings of the 13th International Workshop on Security Protocols (2005)

[16]. Buyya, R., Murshed, M.: GridSim: a toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing. Journal of concurrency and computation practice and experience 14(13-15), 1175–1220 (2002)

[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]. Slamanig D. More privacy for cloud users: privacy-preserving resource usage in the cloud. 4th Hot Topics in Privacy Enhancing Technologies (HotPETs), 2011

[19]. Slamanig D. Efficient schemes for anonymous yet authorized and bounded use of cloud resources. Selected Areas in Cryptography, LNCS, 2012, 7118: 73-91

[20]. Cloud security alliance. Security Guideline for Critical Areas of Focus in Cloud Computing V3.0, 2011.