Cloud Intelligent Track – Risk Analysis And Privacy Data Management In The Cloud Computing

M.R.Aswin
Department of Information Technology
Sri Krishna College of Technology
Coimbatore, India
aswram23@gmail.com

M.Kavitha
Department of Information Technology
Sri Krishna College of Technology
Coimbatore, India
kavi_ciet@yahoo.co.in

***Abstract*— Cloud computing is a computing platform with the backbone of internet to store, access the data and application which is in the cloud, not in the computer. The biggest issue which should be addressed in cloud computing are security and privacy. Outsourcing data to other companies worries internet clients to think about the privacy data. Most Enterprise executives hesitate to use cloud computing system due to their sensitive enterprise information. This paper provides data integrity and user privacy through cloud intelligent track system. This paper discuss about the previous experiment done on the privacy and data management. The work proposes the Architecture or system which provides intelligent track in Privacy Manager and Risk Manager to address privacy issues which rules the cloud environment.**

Keywords- Cloud computing; Privacy Manager; Riks Manager; database management; intelligent track.

I. INTRODUCTION

Cloud computing is anywhere and everywhere. Lets pick up any technical magazine or visit almost any IT website or blog and we will be sure to see talk about cloud computing. A survey done in 2006 which says if a question posted to different professions as what is Cloud computing? The survey says that we get different answers from different professionals. Cloud computing gives practical cost benefits such as investment cost and operating cost and can transform a data from one environment to other priced environment. Still security plays a major part in Internet, when we are using it to send sensitive information between enterprise parties. Information Technology is blooming in the areas of mobile computing, pervasive computing or ubiquitous computing, and dominant cloud computing. Cloud Providers offer services that can be grouped as saas: software-as-a-service [2] [9], paas: platform-as-a-service and iaas: infrastructure-as-a-service.

Now a day's most of the Enterprises deploy applications on Public, Private or Hybrid clouds. Public clouds are maintained by third parties as the charge for service. Private clouds are built exclusively for a specific enterprise application or in a private sector to meet enterprise needs. Hybrid Clouds is the combination of both public and private clouds. Currently the most important problem in the cloud computing is security, privacy and energy efficiency issues. SUN has recently deployed a platform the Sun-Open-Cloud-Platform [10] under Commons license. In 2011, hacking groups like Lulzsec and Anonymous provoked an Internet firestorm by hacking major Web sites like Fox.com and online services like Sony's PlayStation Network. Millions of user accounts were compromised. Usernames, passwords, home addresses and credit card information -- lax Web site security often allows hackers easy access of personal information. We can blame corporations for poor security and hackers for maliciously attacking Web sites, but there's a third party often at fault in these attacks, ourselves, the users.

If a client tries to access data and applications irrespective of location he has a possibility of compromising on privacy data. Cloud computing Providers are in need to find an alternative ways to protect client privacy information. One way is to use authentication techniques [1] with the help of user names, passwords or with secured credentials. Another way is to employ an authorization process format such as each user can access the data and applications relevant to business or need. The question of the customer is what is the security for our data? In this issues lots of researching is going on. This paper introduces little idea of privacy for the data through the data management. This paper introduces these ideas with the help of privacy manager and risk manager. Privacy manager deals with data storage and generating key for the data.

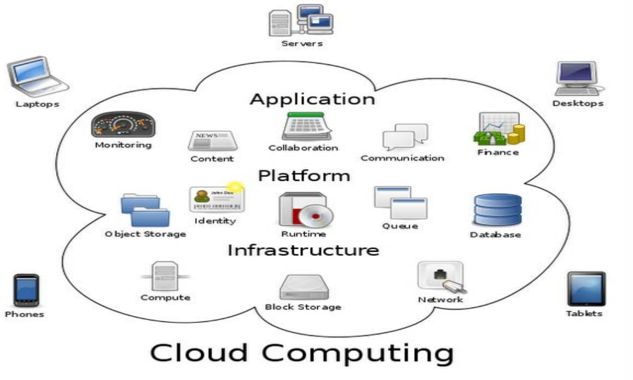


Fig 1 Overview of Cloud computing

ISBN: 978-1-4673-1601-9/12/$31.00 ©2012 IEEE

Risk manager deals with risk availability in the data that received from the cloud database. The fig 1 is given in the Google for the cloud computing architecture. To implement public-key encryption the best way to use digital certificates, which is basically a unique piece of code which says that communication is trusted, where certificate authority plays a major role in digital certificate verification**.**

LastPass is a password management utility that locks all of your unique passwords behind one master password. That means you can create separate logins for e-mail, Facebook, Twitter, cloud storage. LastPass is just one example of a cloud-based service that makes managing data on the Web easier. When it comes to preserving your important pictures and files, finding the right backup services is key.

II. RELATED WORK

As cloud computing provides lot of advantages over service computing and pervasive computing [12]. Different dimension like storage, interface, data type synchronization are compared. Qualitative comparison framework is given by Mie. Though Siani [9] deals with privacy in cloud computing but his system does not contain any type of solution for the risk in the data from cloud.

A Good database management Technique is provides by Bo peng and Dean [2] [6] in the form of Tplatform and Map reduces. Map Reduces Technique uses different mappers in cloud to manage database. But still a problem arises when mapping is done. Tharam Dillon, he gives a clear differentiation and relationships about Cloud computing, Service-Oriented Architecture, pervasive computing and Grid computing [7]. Where he gave a complete comparative study on few challenges towards Cloud computing. Young Choon Lee, has addressed scheduling problem as a result he presented two sets of profit-driven service request [1] scheduling algorithms which gives best results compared to other scheduling techniques implemented.

III. PROPOSED ARCHITECTURE- CLOUD INTELLIGENT TRACK

A. *In Private Cloud*

In this proposed solution, data's of the user are not saved directly in the database of the cloud. If it is saved directly to the cloud's database without providing any security or privacy measure, then it is very easy to other users who do not know it to hack or use it. So in this proposed solution there will be a privacy manager in both client side and also in the cloud side. Cloud intelligent system uses privacy manager and risk manager. Privacy manager implements an algorithm which is used to separate the data and store those data in a random location. And those locations also will be saved in the privacy manager database. When the request is sent by the client for data processing, the algorithm will recollect the data's from the cloud database in accordance to the locations present in the privacy manager of the client side. Then those data will arrange in a proper way and then they produced to the client or user. In this transmission, data from client to cloud may cause damages to the data. To avoid those damages in privacy manager, it will contain risk manager where amount of the risk in the data will be calculated. With that calculated risk, we can avoid risks in the data which is from the cloud database. In case of risk the request is again resend to the cloud server. The private cloud architecture is given in the fig 2. The fig 2 depicts the intelligent cloud system implement with privacy manager and risk manager.

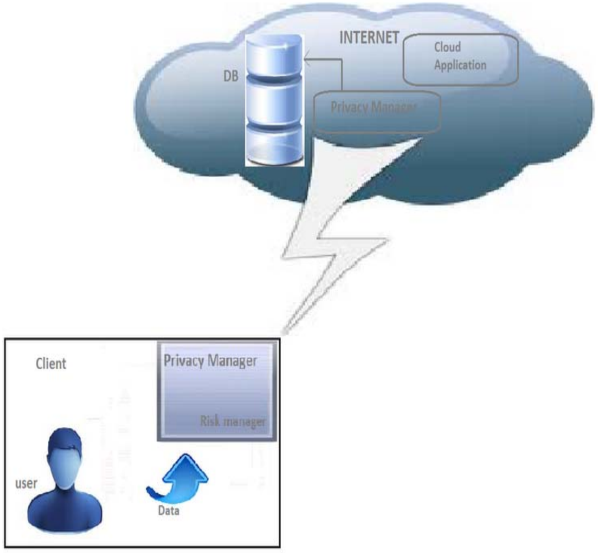


Fig 2 Architecture of Intelligent Private Cloud

B. *In Hybrid cloud*

When issues comes for hybrid cloud data's are not directly transmitted from private cloud to public cloud. Here comes the privacy manager which resides in private cloud side, not in the public cloud. If there is any need of updating the database management in the private cloud side means, the updating can be done through the private cloud an intelligent cloud.

The hybrid cloud architecture is given in the fig 3. Fig 3 depicts the private intelligent cloud environment which communicates with public cloud where secure data can be transmitted with risk analysis. This is how secured data management or data transaction can be done via secure intelligent track. This helps each client in the private side to update their data by their own. If they need to secure their data within the private cloud means. They can create or generate their own keywords for the data which is to be secure.

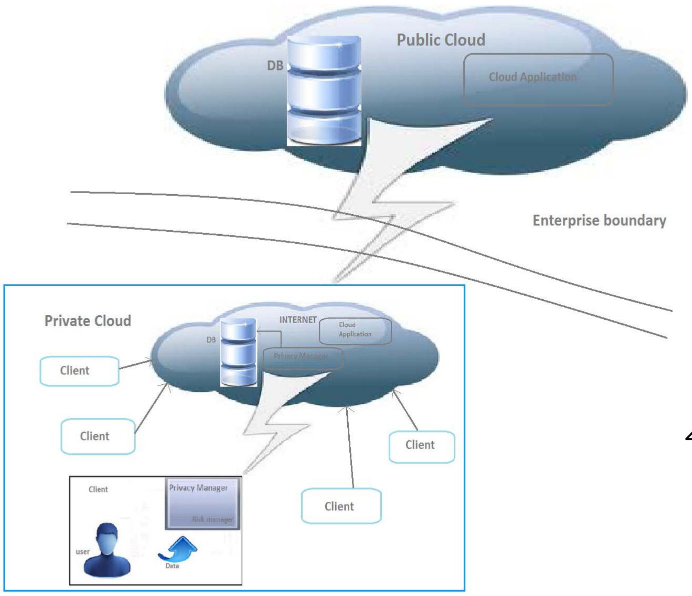


Fig 3 Architecture of the Hybrid Intelligent Cloud

Each updating in privacy manager can only be done through the server of the private cloud. There will not be any kind of direct link between the client machines. This gives security to private cloud side. In this hybrid cloud, data's from the public cloud will not directly reach the client. It should pass through the privacy manager of both the private cloud and client machine, so those data will be secure.

C. Functionality of Privacy Manager

Privacy manager does the main operation while the client transmitting the data to the cloud database. Each client machine consists of own privacy manager. But they are updated with the help of the server in the cloud. So each cloud does not have direct contact with other client to provide the security in the private cloud. It consists of functionality like,

- Working process
- Encryption
- Decryption
- Memory management
- Keyword generation
- Risk manager

D. Working Process

Fig 4 depicts the request from client to cloud, where a segmented data in encrypted and send via the communication protocol to cloud. Fig 5 in turn depicts the response from cloud to client on a requested data. This process verifies the corrected data for proper security.

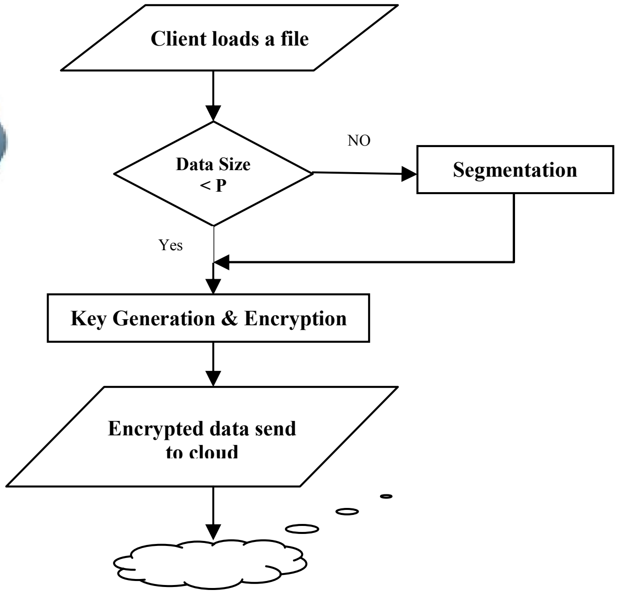


Fig 4 Working process of Data transfer from Client to Intelligent Cloud

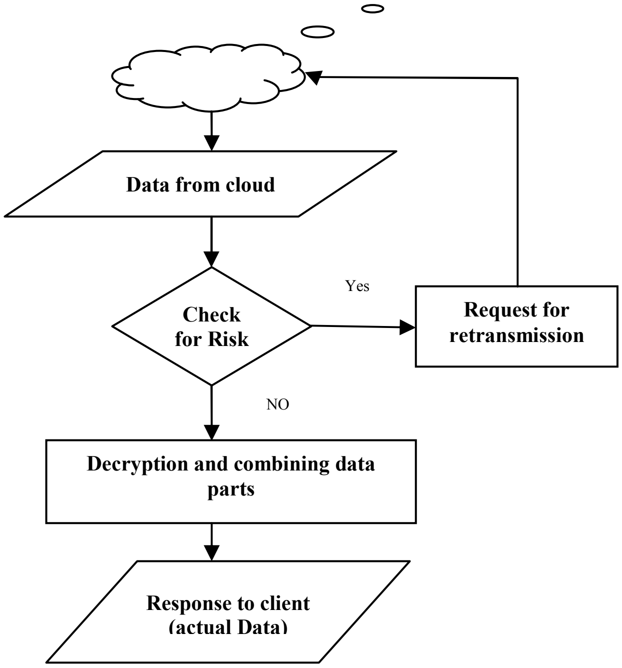

Data from cloud
Check for Risk
Yes
Request for retransmission
NO
Decryption and combining data parts
Response to client (actual Data)

Fig 5 Working Process of Data Transfer from Cloud to Client

E. Encryption

In this phase of the privacy manager, the data's given by the client to be stored in the server database is encrypted with relevant public key. After the process of the Encryption in the privacy manager in the client side, the data is transmitted to the database of the cloud. This keyword is stored in the privacy manager itself to decrypt the data from the cloud. The process of the Encryption is done only when the data is in large size. This paper uses the most popular algorithm: RSA algorithm for Encrypting data.

Encrypted data = E (A, k1),
Encrypted data=E (S1, k1) +E (S2, k2) +E (S3, K3),
Where,

E= Encryption,

A= Data sent by the client,

S1, S2, S3= Segmented data which is equal to the fixed data size.

k1, k2, k3= key word,

The diagrammatic representation of Encryption is given in the fig 6.

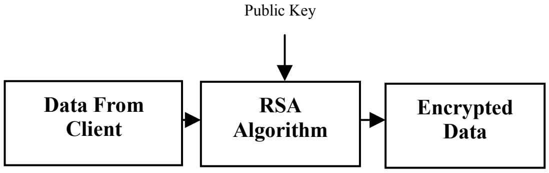


Fig 6 Encryption

F. Decryption

In this phase of the privacy manager, the data's that is requested by the client from cloud database. The data will come to the privacy manager, as it is from the database of the cloud. When it reach the privacy manager of the client, it is combined and removing the key by the private key. Then it sends to the client machine for display.

Decrypted data = D (E (A, k1))
Decrypted data = D (E (S1, k1)) +D (E (S2, k2)) +D (E (S3, k3)),
Where,

D=Decryption,

The diagrammatic representation of Decryption is given in the fig 7.

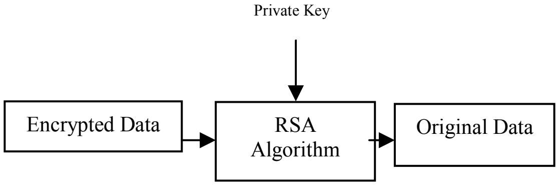


Fig 7 Decryption

G. Memory Management

In this phase of the privacy manager, the management of the data is performed. According to my idea the data from the client is separated into many segments, it is stored in random location and if the data comes to the client it is re-joined to present. These operations are done in the management phase.

- Data are separated into many segments and stored in the random location in the database of cloud.
- Data's segments of the location is stored in the database of the privacy manager in client machine
- With the help of the stored location, the data are collected and re-joined in the privacy manager.

These are the three processes done in the memory management phase of the privacy manager.

H. Keyword Generation

In this phase of the privacy manager, for the data which is in large size key word is generated in privacy manager. These keywords are stored in the database of the privacy manger itself to decrypt the data when it returns to the client. The keyword generation is not only done by the privacy manager and also can be done by the user itself. The most commonly know RSA algorithm is used.

Generation of key using RSA algorithm:
Let p and q be the two prime, are of almost equal in size. An integer or public exponent e, 1<e< phi where
Gcd (e,phi) =1.
The secret exponent d, i< d< phi where
ed =1(mod phi).
n=pq; Φ (phi) = (p-1) (q-1);

Here public key is k1= (n, e) and private key is (d, p, and q).

I. Risk Manager

In this phase of the privacy manager, the data which is from the cloud is checked for the risk. Checking for the risk in the risk manager is done with the help of the cyclic redundancy check algorithm. The operations done in the risk manager phase are,

- When the data entered into the risk manager it starts checking for the error in the data with the help of the cyclic redundancy check algorithm.
- If received data has more number of risks, then the data is rejected and request is sent again.
- If the received data has no error, the data is accepted in these phase.

These are the functions that performed in the risk manager phase of the privacy manager. Here the diagrammatic representation of the risk manager if given in the fig 8.

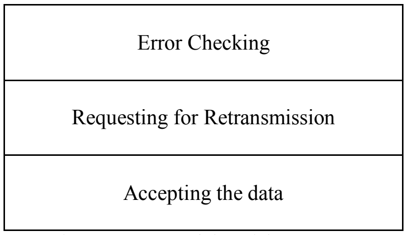


Fig 8 Structure of the Risk Manager

These are the six phases performed in the privacy manager. Here the diagrammatic representation of the privacy manager if given in the fig 9.

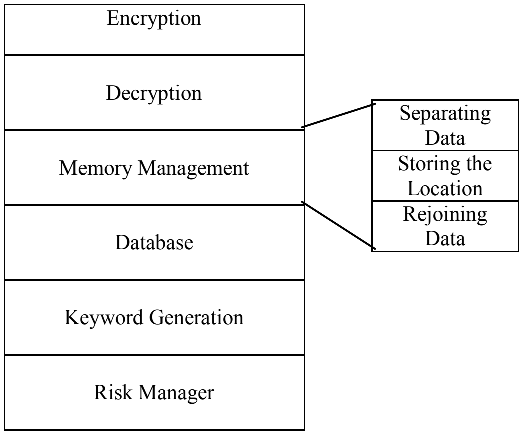
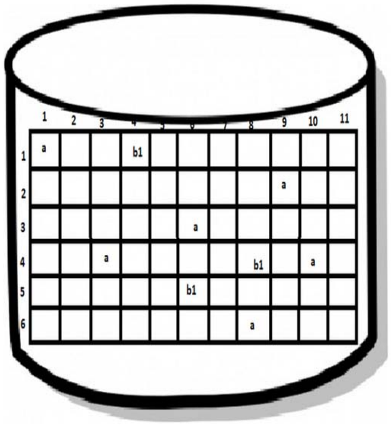


Fig 9 Functional Structure of the Privacy Manager

J. Structure of Database

In this proposed solution, database structure act main role. The database structure contains the structure of the matrix format. In this, privacy manager stores the data in the random locations and store them in their database. For example in the below diagram, data A is segmented into six and they stored in the random location like (1, 1), (2, 9), (3, 6), (4, 3), (4, 10), (6, 8). These location details are stored in the database of the privacy manager. In need of data, the segmented data is brought to the privacy manager, combine and given to the client. In the same diagram, data B is stored with the key1 in random location. Because data B is larger in size, in this case data are encrypted and decrypted. The memory location the data B is (1, 4), (4, 8), (5, 6).



	1	2	3	4	5	6	7	8	9	10	11
1	a			b1							
2									a		
3						a					
4			a					b1		a	
5						b1					
6								a			

Fig 10 Server Database Architecture

K. Proposed Algorithm

```
Privacy Manager
        Input: Request to any type of data from client (A)
        Output:  display requested data
  1.  Initialize the P (packet or data size) value.
  2.  If (size(A)<P)
            Data=E (A, k1)
  3.  Else     //segmentation
  4.  A=S1+ S2+ S3
        Where S1, S2, S3 packets size is P
  5.  Data= E (S1, k1) +E (S2, k2) +E (S3, K3)
  6.  Store the data in the cloud and store the location in
      privacy manager database.
  7.  And when the client request for a data.
  8.  Collect the packets from the cloud and bring to the
      privacy manager.
  9.  Check for the risk in the risk manager using the CRC
      algorithm
  10. If (PAK=1)
        Where PAK is the no of packets from the client
  11. Data=D (E (A, k1))
  12. Else
        Data = D (E (S1, k1)) +D (E (S2, k2)) +D (E (S3,
        k3))
  13. Combine the packets to form a data and deliver to the
      client.
```

```
Risk Manager
    1.  Rem = Data % key
    2.  Request=REQ (Rem+ Data)
    3.  Response=RES (Rem+ Data)
    4.  If (Response %key=0)
    5.  Accept the data
    6.  Else        //consists of risk
    7.  Send request for retransmission.
```

L. Implementation Details

A sample part of database is provided; consider client is need of a text file flower.txt which is saved somewhere in cloud table which is access as follows. SQL query for processing:

```
LOAD DATA LOCAL INFILE '/path/flower.txt' INTO TABLE Data;
LOAD DATA LOCAL INFILE '/path/flower.txt' INTO TABLE Data LINES TERMINATED BY '\r\n';
INSERT INTO <table name>VALUES ('first name', 'middle name', 'last name','age','1984-11-2', NULL);
SELECT * FROM table name;
DELETE FROM table name;
LOAD DATA LOCAL INFILE 'flower.txt' INTO TABLE Data;
```

```
UPDATE Data SET birth = '1980-10-3' WHERE name = 'Shiller';
SELECT * FROM data WHERE birth >= '1987-11-6';
SELECT * FROM Data WHERE species = 'X' AND sex = 'm';
SELECT * FROM Data WHERE (name = ' xxx' AND sex = 'm') OR (name = ' yyy' AND sex = 'f');
SELECT * FROM Data WHERE name = 'shiller';
SELECT name, age  FROM table name;
SELECT name, age FROM Data ORDER BY birth;
SELECT name, age, birth FROM data ORDER BY name, birth DESC;
```

Data calculation:

```
SELECT name, birth, CURDATE(), (YEAR(CURDATE())-YEAR(name)) (RIGHT(CURDATE(),0)<RIGHT(name,9)) AS age FROM Data;
```

A sample screen shot for data retrieval is shown which gives the basic idea of how the intelligent cloud system works. After possible credential verification process the user is allowed to upload a file as given in fig 11. Later the file goes to the cloud through privacy manager and risk manager where our intelligent track system acts. This proposed intelligent cloud system can be implemented by setting a Eucalyptus cloud environment and by using Aneka tool to import java packages to resolve the issues.

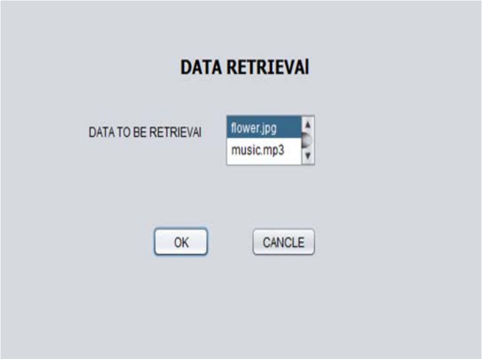


Fig 11 Request to Cloud

Fig 11 depicts the file request from client to server in cloud. The request which undergoes lot of process to fetch a file from cloud database. The intermediate process which takes care of Risk and privacy management of database. As a result Fig 12 shows the requested data.

Fig 12 Response from cloud

IV. CONCLUSION

This paper implements intelligent cloud with techniques to solve the privacy and data management problem. This proposed solution can be applied to current cloud computing process. This research work carried out gives enhanced performance hence can be used for many applications like online banking, credit card transactions, where large and sensitive number of data sets need to be handled.

REFERENCES

[1] Bertino E Ferrari E "Secure and Selective Dissemination of XML Documents" In Proceeding of TISSEC, ACM, pg. 290-331 2002

[2] Bo Peng, Bin Cui and Xiaoming Li, "Implementation Issues of A Cloud Computing Platform", Department of Computer Science and Technology, Peking University.

[3] Boneh, D., Franklin, M. "Identity-based Encryption from the Weil Pairing" in CRYPTO 2001. LNCS, vol. 2139, pg.213—229. Springer, Heidelberg 2001.

[4] Casassa Mont, Pearson, Bramhall P: "Towards Accountable Management of Identity and Privacy Sticky Policies and Enforceable Tracing Services" in IEEE Workshop on Data and Expert Systems Applications, pg. 377—382. IEEE Computer Society Press, Washington DC -2003.

[5] Cong Wang, Qian Wang and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", Department of ECE, Illinois Institute of Technology.

[6] Dean J. Ghemawat S " Map Reduce: Simplified data processing on large clusters" in Communications of the ACM, Vol. 51, No. 1 2008

[7] Gritzalis D, Moulinos K. Kostis K.: "A Privacy-Enhancing e-Business Model Based on Infomediaries" in MMM-ACNS 2001, LNCS 2052, pg. 72–83. Springer Verlag Berlin Heidelberg 2001.

[8] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Elaine Shi, Jessica Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", PARC Fujitsu Laboratories of America

[9] Siani Pearson, Yun Shen and Miranda Mowbray, "A Privacy Manager for Cloud Computing", HP Labs, Long Down Avenue, Stoke Gifford, Bristol BS34 8QZ, UK.

[10] "Sun Microsystems Unveils Open Cloud Platform," 2009.

[11] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", Digital Ecosystems and Business Intelligence Institute Curtin University of Technology, Perth, Australia

[12] W.K.Chan, Lijun Mei, T.HTse, "A Tale of Clouds- Paradigm Comparisons and Some Thoughts on Research Issues", IEEE Asia-Pacific Services Computing Conference pg: 464-469 2008.