A Hybrid Cryptographic Technique for Secured Authentication in Cloud Computing

Juber Mirza
PG Scholar
Institute of Engineering & Technology DAVV Indore

Meena Sharma
Professor
Institute of Engineering & Technology DAVV Indore

ABSTRACT
The cloud infrastructure development and service distribution is a complex task. A number of members are contributing in this task such as clients, intermediate service providers and the data centre owners. In such kind of scenarios the infrastructure providers are distribute their service by the help of intermediate servers or vendors. Due to this the quality of service, trust, security and privacy of the data and their owner is a key issue of management. Therefore a secure and trust worthy environment is need to be created for improving the data owner trust on the primary service providers.

In this presented work the key focus of the study is placed on the server security and the user trust management. Therefore the proposed technique involves the development of secure cryptographic cloud. The cryptographic cloud is implemented with the help of a hybrid cryptographic technique which involve the Data Encryption standard (DES) encryption technique for ciphering data and for key exchange the Diffie Hellman (DH) algorithm is implemented. Further for more improved security the integrity check is also implemented with the help of Message Digest (MD) 5 hash generation algorithm. After implementation of the cryptographic cloud the trust management between the primary service provider and brokers are need to implement for managing the end client trust on primary service provider. Therefore a two factor trust computation technique is proposed using the server rating and the number of request failures. This trust value is help to regulate the quality of service offered by the primary service provider.

The implementation of the proposed technique is performed with the help of JAVA technology and their performance is reported with the help of space and time complexity. According to the experimental results the proposed technique offers more secure environment and with less computational overheads.

Keywords
Cloud Security, Trustworthy Cloud, Privacy on Cloud, Secure Cryptographic Cloud, Transparency

1. INTRODUCTION
The cloud computing is a new generation computing technology. That is used to handle a significant amount of data and job processing request. Therefore the cloud is a huge computational and storage infrastructure which is works in saleable and efficient manner. But due to the huge amount of data, cloud service providers utilize the data outsourcing concept for reducing the maintenance cost and effort. But the data centers and their providers need reliability, availability, and efficiency for data access and during user data retrieval. Therefore the data centers replicate the data into more than one place for reliable and efficient access.

On the other hand during the data processing and updates a significant amount of computational resources are consumed. Thus a technique is required to handle the authentic update request. Therefore a technique is required that is able to distinguish the genuine update request. Thus the proposed work includes a technique of cryptographic cloud demonstration by which the data in the third party server is placed in secured manner. Additionally the solution needs to incorporate a technique by which the trusts among user data updates are managed, by which the frequent updates and unwanted computational losses are preserved. The proposed trust computation technique is based on the multi-factor trust parameters.

Cloud computing is a technology that enables the remote user to experience efficient computing and digital data storage solutions. Therefore a number of individuals and organizations utilize the cloud hosting services. The cloud service providers offer the scalable storage solutions therefore it is required to make collaboration with other service providers or for service distribution the intermediate service providers are also associated with the service providers. In this concept the primary service providers are offered the storage services through the brokers or intermediate service providers. Therefore the primary service provider is worried about the quality of services offered by the intermediate servers.

Therefore in this presented work a cloud storage service is demonstrated using the primary and secondary service providers. Here the primary server denotes the primary service provider and secondary server denotes the intermediate service provider. Additionally to keep in track the security and the authenticity of data and service access a trust management technique is offered. The trust management technique helps to identify which service provider is not working well or compromised with the client's expectations. Therefore the user rating and service failures are used for computing the weighted trust for service delivery.

In addition of that for securing the data and manage trust among the service providers and the end clients the proposed work involved a formulation of cryptographic approach for preparing the cryptographic cloud. That cryptographic cloud is used to preserve the data and their sensitivity during the data preservation, data access and storage in other third party servers. In this section the overview of the proposed security and trust management technique is provided. Additionally in the next the problem identification is observed from literature survey then in next section the proposed methodology for cryptographic security and trust management technique is provided using hybrid cryptographic technique.

2. PROBLEM DOMAIN

The cloud is a diverse domain of computing and data hosting, data is continuously flowing and changing their place in the cloud infrastructure. Therefore some problem addressed after studying reference papers first one is most of the authentication and verification techniques are time consuming, second to the best of our knowledge there is no existing integrity verification scheme can provide authentication on transmitted data. Lack of security during data exchange and updates on multiple blocks is another major problem and last one is the amount of data is huge thus auditing and access is very complex on data outsourcing.

3. PROPOSED WORK

The proposed work includes two different major goals to achieve first the secure storage unit on which the data is hosted in cryptographic manner. Additionally during the service distribution need to manage the trust between two servers. Therefore the formulation of the proposed technique performed on two modules.

3.1 Cryptographic Cloud

The cloud storage is a diverse for managing the data, therefore the place and availability of data can be depends on the nature of traffic generated for storage needs. Thus need to preserve the data sensitivity and privacy from others.

Therefore cryptographic techniques are used for securing the data and the data owner's privacy. In this section a cryptographic technique is used for securing the data, figure 3.1 shows the proposed cryptographic model for securing data during the network data transmission.

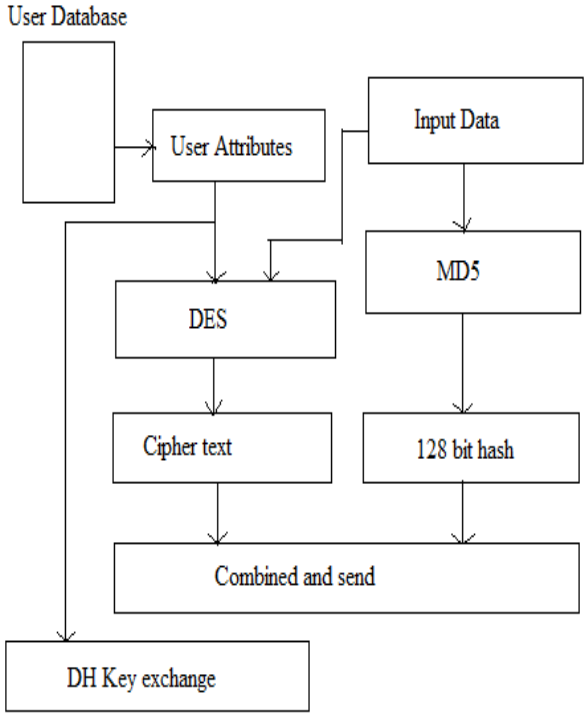

Figure 3.1 Proposed cryptographic technique

In the above given diagram the proposed cryptographic solution is provided. The cryptographic technique usages the user attributes from the data base to prepare the key for encryption. The selected key and data is passed on the DES algorithm for encryption of data. The DES algorithm processes the data using the selected user attributes and generates the cipher text. On the other hand the input data for transmission is processed using the MD5 algorithm. This algorithm generates 128 bit hash code for the input data. In further the MD5 hash and the generated cipher text is combined for transmission and the selected attribute or the key for recovery of data is exchanged to the server using the DH (Diffie-Hellman key exchange) process.

At the receiver end the cipher and the 128 bit hash is separated and the obtained key using Diffie-Hellman key exchange process is used to recover original data. Therefore the obtained key and cipher text is processed using the DES algorithm for the original data recovery. The recovered data is again processed using the MD5 algorithm for generating the 128 bit key. This generated 128 bit is compared with the server obtained 128 bit key. If both the keys are similar then data is accepted otherwise the data is rejected.

3.2 Trust Management

This section provides the understanding about the system for managing the trust between the primary server and the secondary server. Because the secondary server promises to distribute the efficient and secure manner to distribute the service of primary server therefore a trust value is computed between the primary server and secondary server. If the secondary server found untrusted for the primary server then the primary server block the request of secondary server. In order to compute the trust the following formula is used:

$$Trust = U_r * w_1 + F_c * w_2$$

Where F_c= number of times the connection refused by the server

U_r= user rating of the server

w_1, w_2= the scaling weights which is used to scale or regulate values of computed trust level.

3.3 Functional Aspects of System

The proposed system architecture is demonstrated in the figure 3.2 the given system contains the essential sub-systems

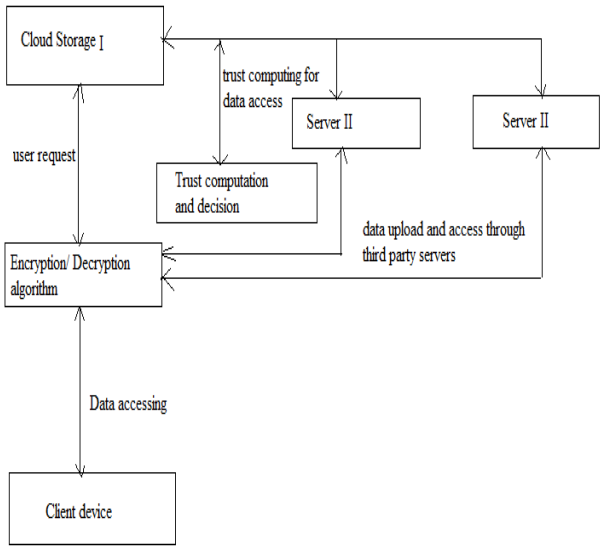

Figure 3.2 System architecture of user data access

for completing the objectives of the work. This section describes the functional aspects of the system. The detailed

understating of the proposed model and their components are given in this section:

Cloud storage: That is a primary cloud infrastructure which is developed to store the data in cryptographic manner. Therefore a hybrid cryptographic technique is prepared and demonstrated in section 4.1 this server offers the service for directly to the end client and similarly for the intermediate servers.

Server II: These servers are intermediate servers, that not have the infrastructure own and they just dealing with the services offered by the primary server. Therefore the client of the primary server or any intermediate server can access their account from any one of the secondary server.

Encryption and decryption: Encryption and decryption is required when the end client needs to preserve their data to server or need to access their data from the server. Therefore each incoming and outgoing request is processed by the encryption technique offered by the server.

Client device: The device by which the server access or preserve the data on the server. Therefore those can a mobile device or any work station for the end user.

Trust computation: During the data exchange between the primary server and secondary server needs to manage the security and trust also, therefore between both the units the trust computation is performed. According to the computed trust the primary server takes the decision of service distribution through their partner server.

4. RESULT ANALYSIS

The experimental evaluation and the system performance is computed and demonstrated in this section. Therefore some essential performance parameters are obtained and listed with their obtained observations.

4.1 Encryption Time

The amount of time required to perform encryption using the selected hybrid cryptographic algorithm is termed as the encryption of the cryptosystem. The encryption time of the proposed and traditional system is demonstrated using figure 4.1 and the table 4.1

Table 4.1 Encryption time

File size (in KB)	Proposed system (Time in KB)	Traditional system (Time in KB)
10	0.473	0.947
50	2.94	5.38
100	5.32	8.47
500	23.42	31.53
1000	47.82	59.41
2000	92.31	142.53
3000	135.33	198.44

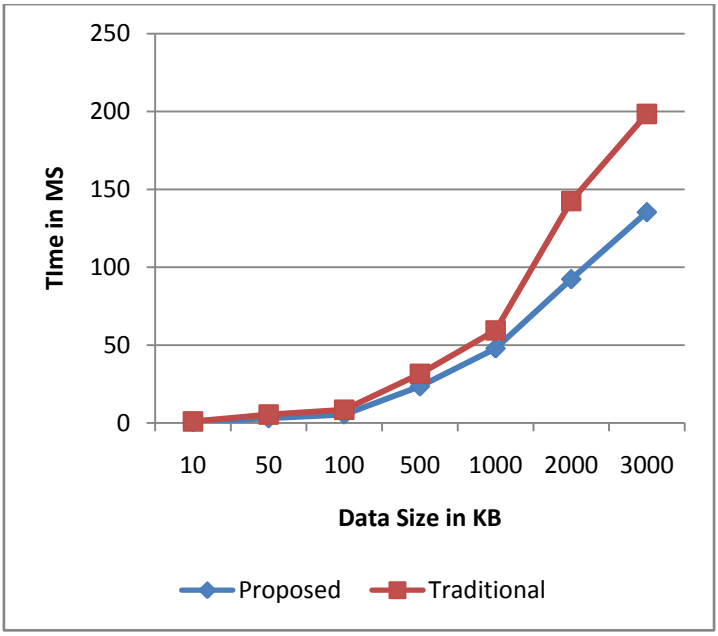

Figure 4.1 Encryption time

In order to show the performance of both the implemented systems the encryption time is reported in figure 4.1 and table 4.1. In this diagram the X axis shows the different file size on which the experimentation is performed and the Y axis shows the amount of time consumed for processing the input file. Additionally the performance of proposed system is given using blue line and the performance of traditional algorithm is given using red line. According to the given results the proposed system consumes less time as compared to traditional algorithm. Additionally the results shows the amount of time consumed is depends on the amount of data provided for execution. But the respective performance of the system shows their effectiveness over the traditional algorithm.

4.2 Decryption Time

The amount of time required to recover the original data from the cipher text is known as the decryption time of the algorithms. The figure 4.2 and table 4.2 shows the obtained performance of the system in terms of decryption time.

Table 4.2 Decryption time

File size (in KB)	Proposed system (Time in KB)	Traditional system (Time in KB)
10	0.331	0.547
50	2.04	3.38
100	4.12	6.21
500	18.14	28.42
1000	34.93	46.52
2000	68.25	112.53
3000	105.39	158.45

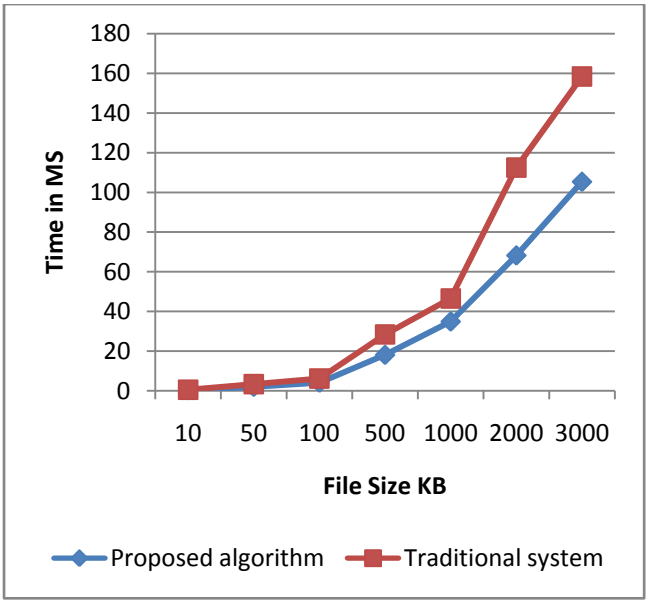

Figure 4.2 Decryption time

To show the performance of both the techniques the blue line shows the performance of proposed algorithm and red line shows the performance traditional algorithms. In given figure 4.2 X axis shows the different file size on which the experiments are performed and the Y axis shows the amount of time consumed. According to the observations the encryption time is higher than the decryption time in both the system, but the decryption time of the proposed hybrid cryptographic algorithm is much adoptable than the traditional algorithm.

4.3 Encryption Memory

The amount of main memory required to execute the hybrid cryptographic algorithm with the input amount of data is known as the encryption memory. The figure 4.3 and the table 4.3 show the encryption memory consumption of the system. In this diagram the amount of main memory consumed is given in Y axis and the file size which are used for experiments are reported at X axis. According to the obtained results the proposed algorithm consumes fewer resources as compared to the traditional encryption technique.

Table 4.3 Encryption memory

File size (in KB)	Proposed technique(in KB)	Traditional technique(in KB)
10	30992	32681
50	30638	33039
100	31028	33924
500	31394	34292
1000	31884	34881
2000	32194	35028
3000	33920	35719

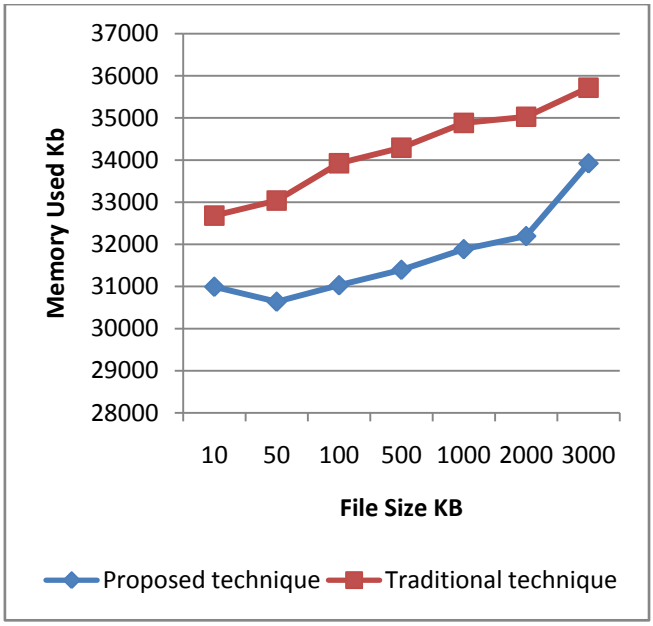

Figure 4.3 Encryption memory

4.4 Decryption Memory

The amount of main memory required to recover the original file from the cipher text is known as the decryption memory consumption. The figure 4.4 and table 4.4 shows the Amount of main memory consumed during the data recovery. In this diagram the X axis shows the different file size used for decryption and the Y axis shows the amount of main memory consumed during the decryption. According to the obtained results the amount of main memory used is higher in the traditional algorithm as compared to the proposed hybrid cryptographic algorithm.

Table 4.4 Decryption memory

File size (in KB)	Proposed technique (in KB)	Traditional technique (in KB)
10	29019	29847
50	29383	30924
100	29981	31947
500	30284	32844
1000	35472	36649
2000	37918	37845
3000	39519	40029

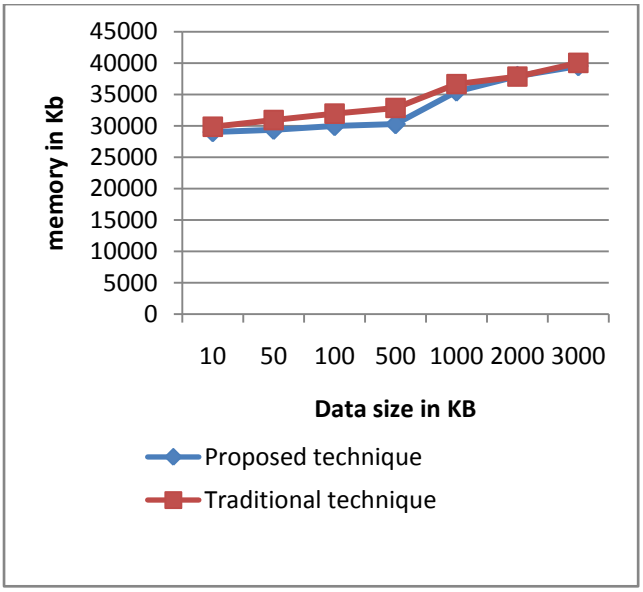

Figure 4.4 Decryption memory

5. CONCLUSION AND FUTURE WORK

The proposed work is intended to deploy a security solution for the cryptographic cloud for securing the data and managing the trust of their users. Therefore a hybrid cryptographic technique and the trust computation technique is proposed and developed in this work. This chapter provides the entire conclusion and summary of the performed work in addition of that the future extension of the work is also suggested.

5.1 Conclusion

The cloud computing is developed for providing the solutions for the scalable storage and the computational services. Therefore in a number of organizations and institutions the cloud computing is utilized. In order to provide the scalable storage solution the cloud service providers follows the concept of the data outsourcing and off sourcing. Additionally sometimes they distribute their service through the intermediate servers. To keep in track security and quality of service of the intermediate service providers the primary infrastructure owner can be worried. Therefore the proposed technique provides an end to end security solution for cloud service providers.

The proposed technique includes the solution for the storage and service distribution for securing the cloud storage the system includes the techniques of hybrid cryptographic cloud. Therefore a DES, MD5 and DH key exchange technique based hybrid cryptographic technique is proposed and implemented. In addition of that the technique enables the primary service provider to compute the trust and Quality of Service of the secondary or intermediate servers. Therefore a two factor (i.e. user service rating and the number of connection failures) are used to compute and manage the trust of the server.

The implementation of the proposed technique is performed using the web based JAVA technology. Additionally for deployment the openshift environment is selected. The openshift technology is a public cloud domain for application and data hosting service. After implementation of the proposed technique the performance of the proposed cryptographic solution is measured and summarized using the below given table 5.

Table 5: Performance summary of Hybrid Technique

S. No.	Parameters	Remark
1	Encryption Time	The encryption time of the system is adoptable and efficient as compared to the RSA based technique
2	Decryption Time	The decryption time of the algorithm is low as compared to encryption time additionally also less than the RSA algorithm
3	Encryption Memory	The memory consumption of the proposed technique is efficient as compared to RSA algorithm
4	Decryption Memory	The decryption memory is also reduced as compared to the traditional cryptographic technique

According to the obtained performance the proposed technique is efficient and secure technique for data storage and retrieval.

5.2 Future work

According to the proposed hybrid cryptographic system and their evaluated results the proposed working model for cryptographic cloud and trust computation during the data exchange is completed successfully. The proposed security solution is efficient technique therefore the technique can be distributable for various other application development, some of the essential domain of applications are demonstrated in this section.

A. The given hybrid cryptographic technique can be prepared by different other cryptographic algorithms in order to reduce the computational overheads more.

B. The technique can be extendable for improving the trust computation technique by including more parameters in the trust computing formula

C. The technique can be implementable for sharing the confidential data for the army operations and the dealer based quality of service checks.

6. ACKNOWLEDGEMENT

It is with immense pleasure that I take the opportunity to express my thanks giving to the great many people who were instrumental in the completion of this project work. The success of this research work would have been uncertain without the help and guidance of a dedicated group of people in our institute IET DAVV Indore. We would like to express our true and sincere acknowledgement as the appreciations for their contribution, encouragement and support. The researchers also wish to express gratitude and warmest appreciation to people, who, in any way to contributed and inspired the researchers.

7. REFERENCES

[1] Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, Jinjun Chen, “MuR-DPA: Top-down Levelled Multi-replicaMerkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud”, IEEE Transactions on Computers (Volume:64 ,Issue: 9)

[2] Torryharris, "Cloud Computing–An Overview", http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

[3] Vaishali Jain, Akshita Sharma, "A Taxonomy on Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014

[4] Balvinder Singh, Priya Nain, "Bottleneck Occurrence in Cloud Computing", National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)

[5] MilenkoRadonic, "Cloud vs. Data Center: What's the difference", http://www.glbrain.com/index.php?r=tool/view&id=2103&toolType=1

[6] V. Abricksen, "A Survey on Cloud Computing and Cloud Security Issues", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622International Conference on Humming Bird (01st March 2014)

[7] SwapnaLia Anil, RoshniThanka, "A Survey on Security of Data outsourcing in Cloud", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013

[8] KratiMehto, Rahul Moriwal, "A Secured and Searchable Encryption Algorithm for Cloud Storage", International Journal of Computer Applications (0975 – 8887) Volume 120 – No.5, June 2015

[9] PradipLamsal, "Understanding Trust and Security", Department of Computer Science University of Helsinki, Finland, 20th of October 2001

[10] Sheikh MahbubHabib, Sebastian Ries, Max Muhlhauser, "Towards a Trust Management System for Cloud Computing", 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)

[11] Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Colouring", Published by the IEEE Computer Society, 1089-7801/10/$26.00 © 2010 IEEE, IEEE Internet Computing

[12] Sidhu and Sarbjeet Singh, "Compliance based trustworthiness calculation mechanism in cloud environment", International Workshop on Intelligent Techniques in Distributed Systems (ITDS-2014), © 2014 The Authors Published by Elsevier B.V

[13] AttaurRehman Khan, Mazliza Othman, Sajjad Ahmad Madani, and SameeUllah Khan, "A Survey of Mobile Cloud Computing Application Models", IEEE Communications Surveys& Tutorials, Accepted For Publications

[14] SmitaSaini, Deep Mann, "Identity Management issues in Cloud Computing", International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 8 – Mar 2014

[15] Eric Kuada, "Towards Trust Engineering for Opportunistic Cloud Services: A Systematic Review of Trust Engineering in Cloud Computing", Aalborg University, Publication date: 2014