International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 3 Issue 3 March 2016

An Implementation of Secure and Trusted Cloud Data Storage for Data Outsourcing

Sangeeta Bamboriya[1], Prof. Jitendra Dangra[2]
Department of Computer Science & Information Technology
Lakshmi Narain College of Technology, Indore, Madhya Pradesh, India[1, 2]
sangeetabamboriya.30@gmail.com[1], jitendra.dangra@gmail.com[2]

Abstract: *Now in these day individuals and organizations are keep their data in digital formats and provide to their clients in on demand manner. Therefore data on hosting servers are increases significantly additionally a number of users try to access their data thus traffic is also increases in these servers. For reducing the maintenance cost of data, cloud managers outsource data to other third party servers to keep preserve data therefore for managing user's data privacy and sensitivity this server usage cryptographic technique. Due to storage and access of data need to regulate storage mechanism. Therefore require to improve user trust during the data outsourced in third parties.*

Therefore a new technique is required to manage user trust when the data is hosted on unknown host. To keep in track the security and privacy on data trust management technique is developed. The proposed solution includes design of cryptographic data storage services and sharing mechanism to demonstrate outsourcing aspects. In addition of that a cryptographic technique is provided to secure data during network exchange. Finally to data storage and access from third party servers a trust evaluation technique is also associated using weighted method.

The implementation is performed using JAVA technology and to ensure authenticity performance of cryptographic technique is evaluated and compared with a traditional cryptographic system. The experimental result demonstrates effectiveness and efficient technique for third party data storage and data exchange in trusted environment.

Keywords: *Cloud Servers, Data Outsourcing, Network Transmission, Cryptographic Cloud, Data Exchange.*

1. INTRODUCTION

Due to frequent use of internet, most of the applications are managed online. The applications are developed in such a manner to serve data and services in 24X7 manners. Thus each and every fraction of seconds a huge amount of requests are generated. These requests are made either storage of data or to find data previously stored. To handle requests in such amount traditional computing becomes out-dated and cloud computing is used with the various applications. The cloud is a huge computational and storage infrastructure to support the huge and frequent changing data requests. To reduce the complexity of data storage and also to reduce the cost of data management the cloud service providers redirect their traffic and data on other third party servers. This concept of resource management on cloud is termed as data outsourcing.

The outsourcing of data needs some technique to improve the security, transparency and trust over the other host. By which the cloud data storage and access becomes trusted on demand service network for end clients. In this presented work a data outsourcing concept with efficient cryptographic security and trusted manner is introduced. Additionally a new concept which improves the data access, sharing, storage is demonstrated. The proposed data model is not a specific kind of security service or infrastructure that provides a generalized framework for hosting and managing the data and entities to manage their personal and sensitive data with the privacy preserving and efficient manner. The key aim of the proposed work is to develop a secure and trusted environment for data storage and sharing services. Therefore the following tasks are included in the entire study.

1. **Investigation of data storage services in cloud servers:** in this phase the cloud computing basics and data storage techniques in cloud are studied. In addition of that how the data is managed, stored and accessed from local and third party storage is also investigated.
2. **Investigation of security in cloud data storage techniques:** in this phase the data hosting and third party storage is discussed in detail, and the issues of privacy and trust management is also studied.
3. **Implementation of secure and trusted technique for data storage and access:** Data storage and outsourcing service is developed in this phase. Additionally using more than one party data sharing and access mechanism is implemented and demonstrated.
4. **Performance evaluation of the proposed technique:** The evaluation of implemented system for finding the performance is performed in terms of time and space complexity with respect to a classically available technique

This section provides the overview of the proposed work and next section provides the understanding about the developed approach for data security in different servers.

2. PROPOSED SYSTEM

The main aim of proposed work is to investigate and develop a secure and trusted environment of data storage services. The proposed approach is enabled for secure data outsourcing and easy of data access. In addition of that technique allow the servers to manage the privacy and trust when data is hosted on third party data storage. Therefore, a cryptographic security using hybrid technique is also proposed and developed. The section provides entire details of the proposed security and trust model.

A. Domain overview

Increasing need of data storage and computational ability leads to develop new and innovative techniques. The techniques needed to manage huge amount of data storage and accessing requests. Because continuously increasing data in cloud data centres need additional management and maintenance cost. Therefore service providers are collaborating with other storage service providers to scale up their services for proper management of data and to reduce the management cost. But the storage service providers are worried about the trust of end user and security of data in third party storages because the primary service providers are responsible to preserve the data sensitivity and data owner's privacy. Therefore that required to develop some solution for the primary server's trust and security issues during data storage and access.

The proposed work introduces a solution for the issues arise during the data parking in third party servers during data outsourcing. Therefore the proposed work is focused on secure and trusted environment development. The proposed technique is not only promises to host data in secure manner that also manages the trust during distribution and access from cloud hosts.

Thus to demonstrate the entire working of concept for data outsourcing and trust management a SaaS (software as a service) for cloud data storage is designed. The developed SaaS provides some basic utilities such as file upload, download and sharing. In addition of that a secondary server is implemented which usages the service of primary server. The secondary server consumes the services owned by primary server and storage space. Using the concept of primary and secondary server the concept of data outsourcing and access control is tried to demonstrate.

In addition of that for improving secure access and data storage management a weighted trust computation technique is incorporated. Basically the weighted trust computed among two parties which are communicating each other. This weight is used here as a threshold for making the secure connection. If weight of a server is not found in a suitable trust label then primary server not provides access to the data.

This section provides an overview of proposed secure and trust computing technique and secure cloud environment. Additionally next section provides the methodology of the system design.

B. Methodology

This section provides understanding and detailed discussion about the proposed solution. The proposed solution provides the solution for the following issues and hurdles.

1. **Data Owner's Identity Management**: Data in cloud storage is moveable due to the concept of outsourcing thus needs to distinguish the data and data owner without harming privacy and sensitivity of data.
2. **Privacy and Security Management**: During data transfer from client to server or server to server need to interact with network. The public network is unsecured due to various attacks i.e. man in the middle attack and others. Therefore need to keep in track security and privacy of data and owner.
3. **Trust Management**: The data can pass through the untrusted hosts or stored in untrusted hosts due to cost issues of maintenance therefore trust computation for servers during data hosting and retrieval is also required.
4. **Data Exchange Security and Data Redundancy Management:** During the data exchange the data is copied in more than one place therefore the redundancy in data increases. Additionally storage overhead is also increases therefore managing the data and security is the key issue of work.

The figure 1 provides the overview of the proposed cloud security solution. The demonstrated system can be divided in two major modules.

1. The implementation of primary server that have the data storage capability and the web services by which the different service and utilities are distributed.
2. The implementation of secondary server that utilizes the storage and other web services from primary server and provides to their own clients.

Using both the servers the involved data exchange process and data access is demonstrated with security and trusted environment. The given outsourcing system prototype involves different sub components to design complete system. Thus in further discussion the entire component based description is provided:

Primary server: that is primary service provider who offers client individuals and other service providers to get the services directly for use or re-distribute the services. Therefore this server offers storage service or hosting services for outsourced data. Additionally that implements the different applications and utilities to demonstrate off sourcing and outsourcing services. The primary server incorporates two major aspects for cloud.

1. **User management:** the primary server manages a data for user records those are getting services directly or indirectly with the primary server. The user or data owner can park their own personal data or organizational data according to their membership with the server and according to their membership policy.
2. **Application and data:** that is a personalize service provided to the client by directly the primary server by which the user can host their data on server and keep in track their data. In addition of that for supporting the different user oriented services some additional utilities are also managed. These utilities offers data upload, download, share and exchange of data to anyone.

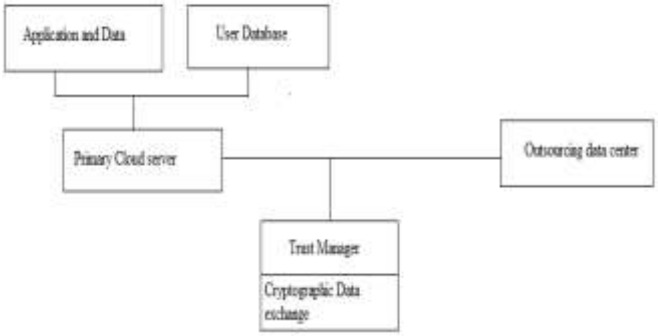

Figure 1 Proposed system

Secondary server: The secondary server is a kind of distributor who leases the services from the primary server and redistributes the services to their own clients as the service provider. To simulate security and trust management the communication among primary and secondary server is used. Additionally the secondary server works with the similar functions as the primary server. The users of secondary server usages the services of primary server for data storage, authentication and data access. During these processes the data owner's need to manage their own data too therefore some applications are implemented to upload, download and sharing of data.

Trust manager: when the two different service providers are communicating for scaling their services. The trust manageris used to compute trust among both the parties (primary and secondary server). If the computed trust value found adoptable then access to the data is provided. Therefore the trust values of the servers are working as threshold for making decision of malicious host or legitimate hosting. Threshold is a kind of value that is statically fixed to the .75 default. Additionally the computed trust values can be varies between 0-1. If the trust values are higher than the fixed threshold then the data outsourced otherwise the connection is refused. In order to compute the weighted trust the following formula is used:

$$T = IP_s * w_1 + U_s * w_2$$

Where:
f_s= number of failures of the secondary server
U_s= user rating and
w_1 and w_2 is used as scaling factor for regulating the contribution of the factors associated with the trust value.

Cryptographic Data exchange: To keep secure and manage the privacy issues of data during network data exchange and storage the cryptographic security is implemented. The proposed cryptographic technique usage the hybrid concept of data security thus blowfish and SHA1 algorithm is used to encrypt and decrypt the data during network transmission and storage. Additionally the MD5 hash keys are used for ensuring the data quality. The figure 2 shows the method of encryption and decryption for securing the data.

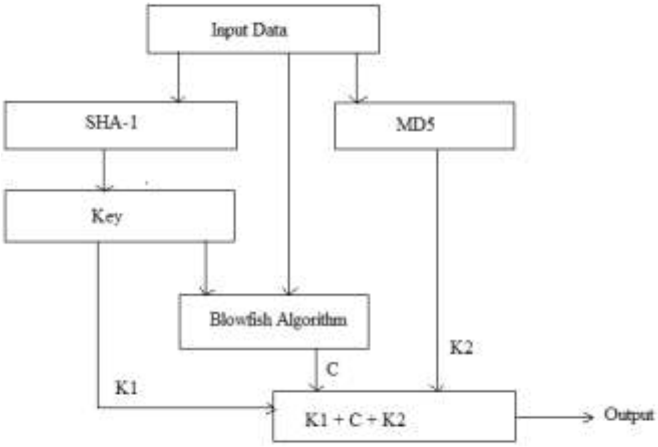

Figure 2 proposed cryptography

The figure 2 provides the overview of the proposed cryptographic technique. in first the input data D is produced to the system as input for upload or download. Using the SHA1 algorithm the hash key that key is the outcome of SHA1 algorithm and termed here as K_1 . In further the blowfish algorithm is implemented which accepts the K_1 and input data as input to produce the cipher text C. on the other hand the data is processed through the MD5 hash function to generate the key K_2. That key is used further at the receiver end to check the data integrity. If the $K_2$is matched with the receiver end key K_2prepared using the received data then the data is accepted otherwise rejected.
To understand about the implemented encryption and decryption algorithm for designed cloud security approach the encryption and decryption algorithm is given using table 1 and 2 respectively.

Table 1 encryption algorithm

Input: original data D Output: cipher text C
Process: 1. $R_d = readData(D)$ 2. $K_1 = GenrateHashSHA1(R_d)$ 3. $K_2 = GenrateHashMD5(R_d)$ 4. $C = Blowfish.encrypt(R_d, K_1)$ 5. Return $C' = K_1$ +C+ K_2

Table 2 decryption algorithm

```
Input: cipher text  C'
Output: original Data D

Process:
1. [$K_1$, C, $K_2$] = extract(C')
2.$R_d = Blowfish.decrypt(C, K_1)$
3. $K = GenrateHashMD5(R_d)$
4.if K= = $K_2$
5. $D = writeintoFile(R_d)$
6. end if
7. return D
```

3. RESULTS ANALYSIS

The section provides the detailed discussion on experimental evaluation of the proposed system and the performance computed. Therefore the evaluated factor based obtained results are listed in this section.

A. Encryption time

The amount of time required to perform encryption is termed as the encryption time of algorithm. The encryption time of the proposed and traditional system computed in terms of milliseconds and demonstrated using figure 3. In this diagram X axis contains the different size of filesby which experimentation is performed and Y axis includes the amount of time consumed to processing the file accordingly. The performance of proposed algorithm is given using blue line and traditional algorithm is given using red color line. According to the reported results proposed algorithm consumes less amount of time with respect to traditional algorithm. Due to observations time consumption is depends on the amount of data. But the respective performance of the system shows their effectiveness over the traditional algorithm. Therefore the proposed approach of cryptography is much adoptable as compared to traditional technique.

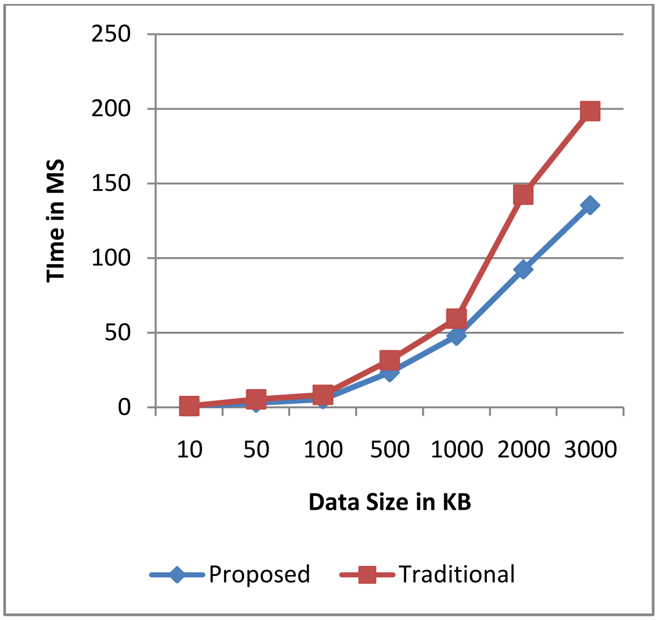

Figure 3 encryption time

B. Decryption time

The amount of time required to decrypt or recover original data from the received cipher text is known as decryption time of algorithms. The figure 4 shows the comparative performance of both the algorithms in terms of milliseconds.

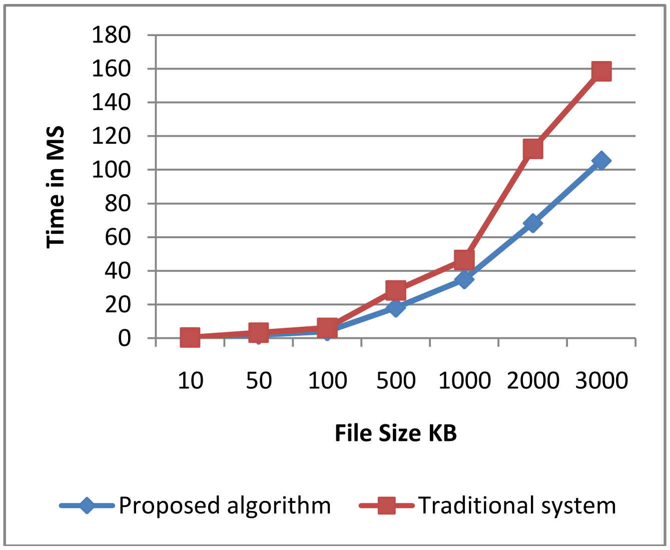

Figure 4 decryption time

The blue line in this diagram shows performance of proposed algorithm and red line shows the performance traditional algorithms. In this figure X axis shows different file size used for experiments and Y axis shows time consumed. According to the observations the encryption time is higher than the decryption time, but decryption time of proposed algorithm is adoptable than the traditional algorithm.

C. Encryption memory

The amount of main memory required to execute the algorithm with input amount of data is termed as encryption space complexity. The figure 5 shows encryption space complexity in terms of KB (kilobytes). In this diagram amount of main memory consumed is given in Y axis and the experimental file size are reported at X axis. In the diagram the blue line shows the memory consumption of proposed technique and the red line demonstrates the memory consumption of traditional approach. According to the obtained performance results proposed algorithm consumes fewer resources as compared to the traditional encryption technique. Therefore the proposed technique is adoptable as compared to traditional cryptographic approach.

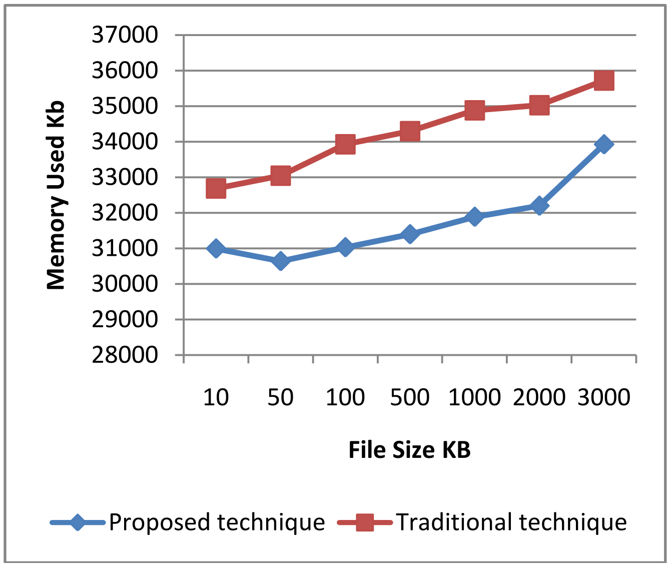

Figure 5 encryption memory

D. Decryption memory

The amount of main memory required to recover or decipher the original data from the received cipher text is known as the decryption memory consumption or space complexity of decryption. The figure 6 shows amount of main memory consumed in terms of KB (kilobytes)at the time of data recovery. In figure X axis shows the experimental file size used and Y axis contains the amount of main memory consumed during the decryption. According to the obtained results the proposed approach consumes less amount of memory as compared to the traditional cryptographic approach. Therefore the proposed technique is much adoptable as compared to the traditional computing.

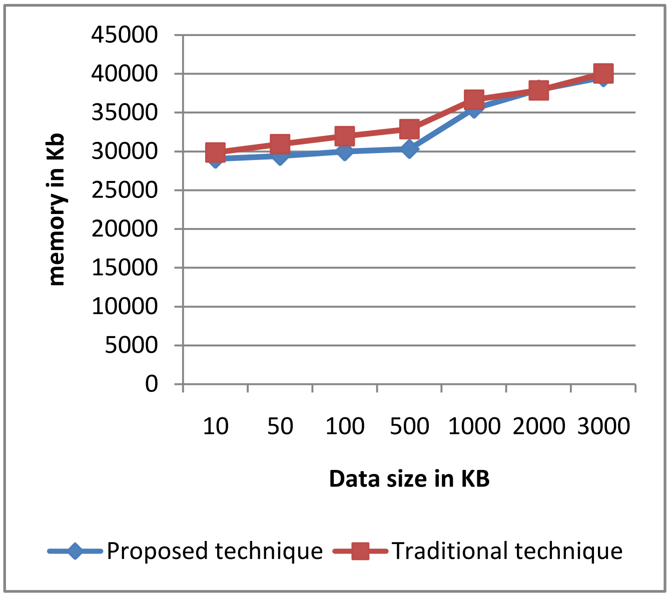

Figure 6 decryption memory

4. CONCLUSION

The study and investigation about cloud infrastructure for secure and trusted storage services for data outsourcing and off sourcing is designed successfully. The summary of entire performed work is included in this section and future extension of the work is also reported.

A. Conclusion

The need of computational ability and storage units is increasing day by day. A number of techniques, methods and algorithms are designed for supporting these needs. The cloud computing offers the solution by scaling the storage and computational services. To scale the service delivery and ensure the QoS cloud data service providers implements various techniques of security and trust management. In this presented work a cloud data management and services distribution concept are investigated. Additionally a solution to ensure reliability and sensitivity in data distribution is introduced.

The proposed approach of data management in cloud servers need to implement two servers for entire security aspect demonstration. First offers to provide the storage services for used to other applications. Additionally secondary server is implemented to consume services of the primary server's for server storage. Therefore the proposed technique contributes on secure cryptographic cloud to preserve data and the data transmitted in public network. Therefore a hybrid cryptographic solution is proposed using the SHA1 and Blowfish algorithm additionally for integrity check the MD5 algorithm is used.

Furthermore the proposed approach provides security of data during the data outsourcing with the help of the weighted trust evaluation of third party host. The weighted trust is used during the accessing and storing data on the server. The trust computation of data request is performed by the characteristics of the third party server and their behaviour with the services delivery.

The implementation of the proposed technique is given using JSP (java server pages) and the public cloud namely Open Shift environment is selected for deployment. After implementation of the system, the performance is evaluated in terms of space and time complexity. The obtained performance is summarized using table 3.

Table 3 performance summary

S. No.	Parameters	Description
1	Encryption time	The encryption time is depends on amount of data to encrypt. Encryption time of proposed technique is efficient than traditional approach.
2	Decryption time	The decryption time of system is less than the encryption time. But decryption time of system is less than traditional system
3	Encryption memory	The memory consumption is depends on amount of data for encryption. The proposed technique enhances memory consumption as compared to traditional technique
4	Decryption memory	Less amount of memory consumed as compared to the traditional approach of cryptography

B. Future work

The key objectives and aim of the work is accomplished for providing the secure and trusted environment for public cloud data storage and outsourcing. The proposed concept is adoptable with minimal resource consumption and optimum trust evaluation. In near future the proposed concept is extended for huge data transfer systems. Additionally that can also be extended with the structured data trust management.

REFERENCES

[1]. Ming Li, Shucheng Yu, Yao Zheng, KuiRen, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013

[2]. Shunan Ma, Jingsha He and FengGao, "An Access Control Model based on Multi-factors Trust", Journal of Networks, Vol. 7, No. 1, January 2012

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

[4]. 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

[5]. 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)

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

[7]. ChittajalluSaiMeghana, "Security and Services Management Aspects of Cloud Architectures", http://www.idrbt.ac.in/PDFs/PT%20Reports/2013/Chittajallu%20Sai%20Meghana_Security%20and%20services%20management%20aspects%20of%20cloud%20architectures_2013.pdf

[8]. V. Abricksen, "A Survey on Cloud Computing and Cloud Security Issues", International Journal of Engineering Research and

Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014)

[9]. 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

[10]. 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

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

[12]. 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)

[13]. Khaled M. Khan and QutaibahMalluhi, "Establishing Trust in Cloud Computing", Published by the IEEE Computer Society 1520-9202/10/$26.00 © 2010 IEEE

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

[15]. Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10/$26.00 ©2010 IEEE

[16]. JagpreetSidhu 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

[17]. C. Bharathi, V. Vijayakumar, K. V. Pradeep, "An Extended Trust Management Scheme for Location Based RealTime Service Composition in secure cloud computing", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), © 2015 The Authors. Published by Elsevier B. V

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

[19]. Zheng Yan, Peng Zhang, Athanasios V. Vasilakos, "A survey on trust management for Internet of Things", & 2014 Elsevier Ltd. All rights reserved.

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

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