International Journal of Advanced Science and Technology
Vol.63, (2014), pp.65-72
http://dx.doi.org/10.14257/ijast.2014.63.06

# TCLOUD: A Trusted Storage Architecture for Cloud Computing

Sultan Ullah and Zheng Xuefeng

*School of Computer and Communication Engineering, University of Science and Technology, Beijing People Republic of China*

*sultan.ustb@yahoo.com, zxf@ies.ustb.edu.cn*

***Abstract***

*The cloud storage provides a least cost means of data storage for the small and large enterprises across the globe. But the main barricade to wide spread adoption of cloud storage is the lake of trust in the technology by its user. The data is stored on multiple servers and the location is concealed from the customers and they are no more in control of the data. This distinctive feature of the cloud storage presents many security and trust challenges. In this paper we present a trusted architecture of cloud data storage. The architecture presents a unique way of secure storage and accessing of data from the cloud data center. It also ensured that only authorized user will be able to access the data. Additionally, if there is any violation of the security parameter at the data center, the data will still be safe i.e. the data will be stored in encrypted form.*

***Keywords:*** *Trusted Storage, Security Challenges, Access Control, Cloud Computing*

## 1. Introduction

A novel architecture of information system is presented in the recent past by the name of cloud computing, which is indeed seen to be a revolution in the history of computing industry. This computing paradigm proffer a unique structure of the utilization of computing resources to business and individual user by a third party companies as alternative to their own computing infrastructure [1, 2]. The customers are not only provided leverage from the requirement of costly hardware equipment by Cloud computing, rather it has reduced the requirement and complexity from customer point of view. Cloud computing present's users the hallucination of unlimited computing resources. The user can utilize computing resources as large, or as diminutive as they required, irrespective trepidation of the maintenance and provision of those resources [3, 4].

The history of cloud computing is endemic with data disclosures either premeditated or unpremeditated. This discloses the risks of privacy and confidentiality of the cloud data storage deployment. The first ever kind of the risk is the unintentional disclosure of data which happens because of the errors in the design of the cloud computing software of the providers. For instance, the non-authenticated users were allowed to view the documents by Google Docs due to a bug [5], whereas the Flicker and Face book have also leaked the private pictures of the users due to flaws [6].

Normally all cloud computing data centers have a central server administration system, which is responsible for the management of overall operations of the data center. Cloud computing provides centralized storage, processing memory, and bandwidth. Due the centralization of computing resources make it attractive targets for insider or outsider attackers. The cloud data service provider's record of protecting data

ISSN: 2005-4238 IJAST

is unsatisfactory. In reality, Twitter made an agreement with Federal Trade commission of the United States due to its sloppy security practices which allowed the attackers to masquerade as any authorize user of the system in 2011 [7]. In addition, several sites have encountered occurrences of security breaches which results in the data lose of users which not only include email addresses but credit card numbers as well [8].

Cloud data service providers encounter huge amount of pressure from government agencies the world over to reveal the private data of the users' when needed. Such as, Google Inc. complies with most of the requests it receives to give the private data of its clients [9]. Additionally, government agencies of several countries have threatened to block blackberry email services if they are not given the right to monitor the users' private data [10].

Sometime the providers of cloud services frequently encompass some money-making inducement from different parties and thus willingly divulge the users' private data, which the users think is private. Google and Face book are two of the service providers which have destabilized their policy and default settings of privacy in order to endorsed new products and services. Moreover, if a provider of cloud service still keeps its promise still the data is at menace [11, 12]. Users have a strong concern over the data confidentiality, security and unauthorized access [13]. This problem became even worse in the case of cloud computing as the user does not have any knowledge about the physical location of the data and control over the data center. A mischievous data service provider can possibly damage users' data by updating, plummeting, transforming, or falsifying segments of the data.

Trust in the cloud is mainly dependent on the security of the service provider. It is a well-known fact that if the system is secure, then it will be trustworthy [11, 14, 15]. In this paper a trusted architecture for data storage in cloud computing which will augment in a whole the security of cloud computing environment is proposed. The cloud data architecture is generally composed of three entities at large, which are the cloud servers, the media and the client. Majority of the research work is done on securing the server but less importance is given to the media of transfer between the client and the cloud environment. A comprehensive architecture is presented in this paper which covers all the aspect. *i.e.*, access control, data transfer through media and finally data storage at the cloud computing data storage center. This will results, enhancing trust on cloud computing.

## 2. Review of Related Literature

As our work is based on providing trusted storage architecture for cloud computing and security is considered to be the first and last component of trust metrics. Therefore we surveyed the literature for previous work on securing cloud storage and found that numerous systems and methods are incorporated to secure the cloud from different perspective. Some of the systems work to develop a trusted cloud environment by providing high level of security. A number of researchers had presented different model to divide and store the user data on different cloud providers as alternative to a single storage service provider.

A trusted computing environment was proposed by researchers for cloud computing in 2010. The platform provides the protection of data by implementing a strong authentication mechanism, and the access is restricted by role based access control method in cloud computing system [14]. A multi – clouds database model was presented as an alternative to single cloud environment by the authors in [16]. The purpose of this model was to safeguard

 

the cloud system from the peril of malevolent insider threat and circumvent the failure of the whole cloud services infrastructure. A novel architecture for authenticated key exchange was proposed with the name of cloud computing background key exchange. It utilizes the internet key exchange and randomness reuse approach for key exchange [17]. Trust management is the prime concern of research for most of the researcher. The model TFMC introduced a trust management model for cloud computing which is based on the fuzzy set theory [18]. The user can use this model in decision making during the selection of a specific cloud service provider to evaluate the trustworthiness of different cloud service providers. The model also provides trust relationship among multiple cloud providers. A unique cost effective and secure model of data distribution is proposed for multi – cloud storage by the authors in [19]. The main idea behind this model is to provide a low cost mechanism of user's data distribution of on available multiple cloud storage providers

The single sign on (SSO) is implemented on the top layer of the cloud computing model. The rationale to this mechanism was to present the user with the best of quality of service including secure storage and availability of data [13, 20]. This method lessens the number of login and increase the security of the overall system.

Privacy preserving and public auditability has been the focus of different research work [21, 22, 23]. The authors proposed a public auditing architecture for cloud computing keeping the privacy preserved [24]. This architecture not only provide the privacy preservation but also support activity like block less verification, public auditability dynamic operation support on data. On the other hand the authors have proved that the architecture presented is insecure due to its incapability to stand against the existential forgery implementing by a known message attack [25]. The authors proposed a protocol for dynamic data auditing on the cloud server that can carry out run time operations on data in [23]. The disadvantage of this scheme is that the data may be disclosed to the auditor as the server sends the linear blocks of data to the auditor.

It is evident from the above discussion that a lot of research has been carried out and still a lot of research works is going on to make cloud computing a secure and trusted technology for the customers. However, several works of this kind are enduring different kind of security issues. Some cannot thwart the illegitimate data access by the cloud service provider while some face the problem of insider malevolent activity. A number of mechanisms are expensive not only in terms of finances, but due to requirement of a time for data processing and the availability of data are affected. So, to avoid these disadvantages the architecture proposed in this paper will allow only the legitimate user to access and store data with confidence. The prime advantage of this scheme is that, it will not only provide security of data at rest (storage at cloud server), but will also provide protection in data during the transmission at transmission media.

## 3. The Proposed Architecture

The proposed architecture is composed of two modules, i.e. the client module and the server module. The general description of the model is given in the following figure.

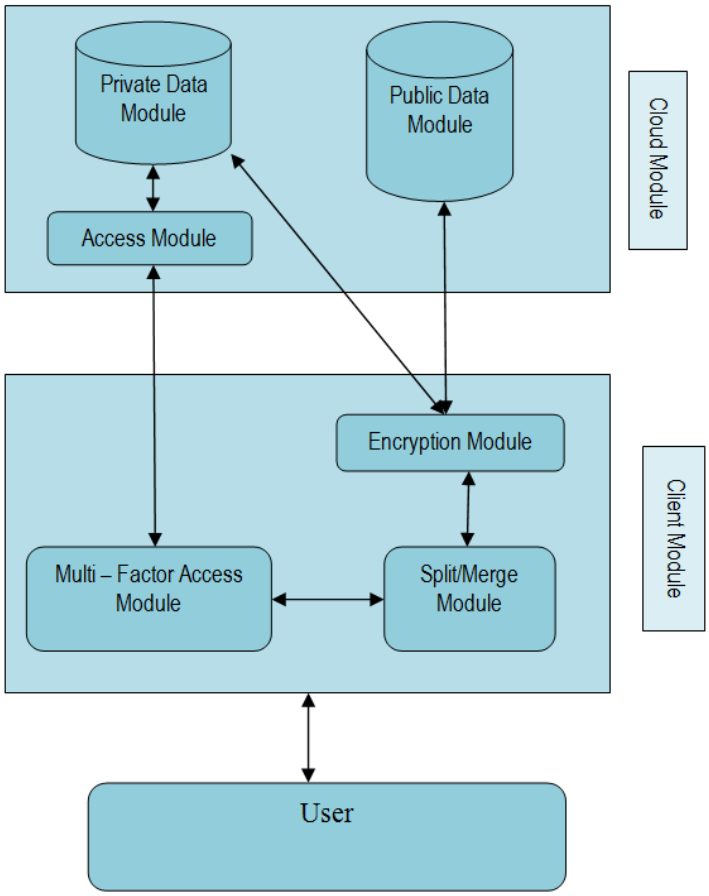


**Figure 1. Block Diagram of the Proposed Architecture**

### 3.1. The Client Module

The client module is mainly composed of three components. The access control component, the split and merge component and the encrypt/decrypt component. The working of each component is explained separately.

#### 3.1.1. The Client Access Control Component:

The access control component is responsible of the authentication and authorization of the cloud user. The simplest mechanism of authentication is a user name and password. But this is too weak method of authentication for cloud computing. The user will login with its user credentials (User Name, Password) and the cloud access control component generates the two session password randomly. One is sent to the user's official email account and the other is sent to a mobile number of the user. The user can be authenticated using both of these session passwords. Once the authentication is complete the access control module will go into the back ground and the rest of the data access and storage will be done through split and merge and encrypt and decrypt components.

 

### 3.1.2. The Split and Merge Component:

After authentication, the user will be granted access to the cloud data storage services. When the client wants to send data, the data will be split first by the split by using the split algorithm. The data can be received and merge algorithm will be used to see the original data form. The split algorithm divide the data into even and odd bits of information and then the merge algorithm reverse the process.

### 3.1.3. Encrypt/Decrypt Component:

After the data is split by the split and merge component, it is then send to encrypt/decrypt component. The encrypt/decrypt component after applying the AES encryption techniques send the encrypted data to cloud storage server, where the data is stored in the public component of the data storage server while the key will be store in the private data component. The same mechanism is applied when the data is requested back from the storage. The key is taken from the private data component and data from the public data component after decrypting the data is given back to split and merge component where the merger algorithm is used to generate the original data.

## 3.2. The Server Module

The cloud server module of our architecture is also composed of three components. These components include the authentication component, the private data component and the public data component. The working of these components is explained as follows.

### 3.2.1 Authentication Component:

The authentication component works in close connection with the private data component of the server module. When the server receives a request for the authorization of data access, it is the responsibility of authentication module to randomly generate two session password and send one of it to user's official email account and the other to the mobile number. The user is then authenticated after checking the session passwords from the user.

### 3.2.2. Private Data Component:

The private data component is not only responsible for the storage of the user's credentials (Login Information). But it is also responsible for the storage of secrete keys needed for the decryption of the data store in the public section of the cloud storage. Only the owner of the data is able to access the private data section of the cloud storage and perform operation like update, delete, append on the data. The user cannot perform data operations on private data section.

### 3.2.3. Public Data Component:

The public component stores the data which will be shared among all the authorized users of the specific data. All the data stored in the public data section will be present in encrypted form. The owner is not only responsible for the creation of data in this component, but also for the different data operations as well.

## 4. Security Analysis of the Architecture

The proposed architecture is simple and secure. The access is controlled by implementing a multifactor and multi-level authentication mechanism [13]. Beside the accessibility, the data is provided multiple level of security by the introduction of split and merge technique before the encryption process which also makes it more secure. As we know that there are a lot of cryptographic algorithms which are considered to be efficient at algorithmic level. In our architecture we used AES Rijendael algorithm for encryption of data files. The overall performance of this scheme is best regarding software and hardware implementation. The algorithm is simple, fast and compact [26, 27, 28, 29].

## 5. Conclusion

The users of cloud technology are increasing rapidly. A trusted architecture of data storage is presented for cloud computing. It not only provides secure access but also provides a trusted mechanism for data transmission through a channel. The multi level access control refrain the unauthorized user from access data while the split and merge technique provide extra security layer before it is encrypted by the encryption algorithm. This process is reversed in the case of downloading the data from the cloud storage server. The suggested architecture increases the level of confidentiality and integrity of the stored data.

## References

[1] L. Yousef, M. Butrico and D. Da Silva, "Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, **(2008),** GCE '08, pp. 1 – 10.
[2] S. Ullah and Z. Xuefeng, "Cloud Computing: a Prologue", International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 1, **(2012),** pp. 1 – 4.
[3] S. Ullah, Z. Xuefeng, Z. Feng and Zhao Haichun, "TCLOUD: Challenges and Best Practices for Cloud Computing", International Journal of Engineering Research and Technology, vol. 1, no. 9, **(2012),** pp. 01-05.
[4] R. L Grossman, "The Case for Cloud Computing", IT Professional, vol. 11, no. 2, **(2009),** pp. 23 – 27.
[5] J. Kincaid, "Google privacy blunder shares your docs without permission", TechCrunch, **(2009)** March, http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/.
[6] Flickr, Flickr phantom photos, **(2007)** February, http://www.flickr.com/help/forum/33657.
[7] U.S. Federal Trade Commission, FTC accepts final settlement with twitter for Failure to safeguard personal information, **(2011)** March, http://www.ftc.gov/opa/2011/03/twitter.shtm.
[8] E. Mills, "Hackers release credit card, other data from stratfor breach", CNET News, **(2011)** December, http://news.cnet.com/8301-27080_3-57350361-245/hackers-release-credit-card-other-data-from-stratfor-breach/.
[9] Google Inc. Transparency Report, https://www.google.com/transparencyreport/userdatarequests/countries/?t=table.
[10] M. Reardon, "India threatens to shut down blackberry service", CNET News, **(2010)** August, http://news.cnet.com/8301-30686_3-20012981-266.html.
[11] S. Ullah, Z. Xuefeng and Z. Feng, "TCLOUD: Inter – Node Communication Model Based on Social Trust Framework for Cloud Computing", Advanced Material Research , vol. 717, no. 2, **(2013),** pp. 688-695.
[12] J. Vijayan, "36 state AGs blast Google's privacy policy change" Computerworld, **(2012)** February, http://www.pcadvisor.co.uk/news/mobile-phone/3340102/36-state-ags-blast-googles-privacy-policy-change/.
[13] **S**. Ullah, Z. Xuefeng and Z. Feng, "TCLOUD: A Multifactor Access Control Framework for Cloud Computing", International Journal of Security and Its Applications, vol. 7, no. 2, **(2013),** pp. 15-26.
[14] Z. Shena and Q. Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, **(2010),** pp. 11-15.
[15] S. Ullah, Z. Xuefeng and Z. Feng, "TCLOUD: A New Model of Data Storage Providing Public Verifiebility and Dynamic Data Recovery for Cloud Computing", Journal of Software Engineering and Applications, vol. 6, no. 3B, **(2013),** pp. 23-28.

 

[16] A. M. Abdullatif, B. Soh and E. Pardede, "MCDB: Using Multi-clouds to Ensure Security in Cloud Computing", IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), **(2011),** pp. 784-791.
[17] E. C. Liu, X. Zhang, J. Chen and C. Yang, "An Authenticated Key Exchange Scheme for Efficient Security Aware Scheduling of Scientific Applications in Cloud Computing", IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), **(2011),** pp. 372 – 379.
[18] X. Sun, G. Chang and F. Li, "A Trust Management Model to Enhance Security of Cloud Computing Environments", International Conference on Networking and Distributed Computing, **(2011),** pp. 244 – 248.
[19] Y. Singh, F. Kandah and W. Zhang, "A secured cost-effective multi-cloud storage in cloud computing", IEEE Computer Communications Workshops (INFOCOM WKSHPS), **(2011)**, pp. 619 – 624.
[20] R. G. Ashish and D. M. Bhavsar, "Securing user authentication using single sign-on in Cloud Computing", IEEE Nirma University International Conference on Engineering (NUiCONE), **(2011),** pp. 1-4.
[21] H. Zhuo, S. Zhong and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability", IEEE transactions on Knowledge and Data Engineering, vol. 23, no. 9, **(2011)**, pp. 1432-1437.
[22] S. Ullah, Z. Xuefeng and Z. Feng, "TCLOUD: A Reliable Data Storage Architecture for Cloud Computing", Advanced Material Research, vol. 717, no. 2, **(2013),** pp. 677-687.
[23] W. Qian, C. Wang, J. Li, K. Ren and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", Computer Security–ESORICS **(2009),** pp. 355-370.
[24] W. Cong, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services", IEEE Network, vol. 24, no. 4, **(2010),** pp. 19-24.
[25] X. U. Chun-xiang, H. E. Xiao-hu and A. Daniel, "Cryptanalysis of auditing protocol proposed by Wang, *et al.*, for data storage security in Cloud Computing", **(2012).**
[26] S. Guha, B. Cheng and P. Francis, "Privad: Practical privacy in online advertising", 8th USENIX Symposium on Networked Systems Design and Implementation (NSDI), **(2011),** pp. 1 – 14.
[27] M. -Z. Dawood, A. R. Khan and S. Akhter, "Advance Encryption Standard", The 18th Saudi National Computer Conference (NCC18), **(2006),** pp. 01 – 13.
[28] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms", IEEE First International Conference on Information and Communication Technologies, (**ICICT 2005)**, pp. 84-89.
[29] S. P. Singh and R. Maini, "Comparison of data encryption algorithms", International Journal of Computer Science and Communication, vol. 2, no. 1, **(2011),** pp. 125-127.

## Authors

**Sultan Ullah**

Sultan Ullah, received MSc and MS degrees in computer science from Sarhad University, Peshawar in 2004 and 2010 respectively. He is currently a PhD candidate at the School of Computer and Communication Engineering, University of Science and Technology, Beijing. His research interest includes Access Control, Network Security, Information Security and Cloud Computing Security. He is a member of the International Association of Engineers.

**Prof. Zheng Xuefeng**

Zheng Xuefeng, was born in 1951, is professor and doctoral supervisor in the School of Computer and Communication Engineering, University of Science and Technology Beijing. His research interest includes Computer Control Systems Development, Computer System Security Analysis, Network Security, Information Security and Distributed Systems Security. He is the senior member of the computer society.