International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 1, No. 2, 2014, pp. 75-81.
ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Offering a Method for Ensuring Data Storage Security in the Cloud Network by Using Kerberos Algorithm

Maryam Zendehboudi[a], Jalil Azimpour [b], Hamed Gorginpour [c]

[a] *Master Student of Public Management, Islamic Azad University, Bushehr, Iran.*

[b] *Master of Educational Management, Islamic Azad University, Bushehr*, Iran.

[b] *Master of Educational Management, Persian Gulf University, Bushehr*, Iran.

Abstract

Cloud computing or computing system of cloud network, is an emerging technology thatdramatically simplified data transition and recovery around the world and reduced substantially the costs associated with the data maintaining. Hence,it can be noted that the cloud computing industry is a lucrative industry in the virtual world. It should be noted that in the use of cloud networking, the users of these networks face some problems such as violation of privacy and security. Since the data security and privacy are the main concerns of users in the use of these networks, the encryption operation can be used as one of the solutions for security and privacy in cloud networks, though this technique itself reduces the system performance. In the present study, we proposed a new model for the encryption, which the operation was carried out through IP and secure passwords receiving. All the cryptographic operations steps in the new model derived from theKerberos algorithm.

Keywords: Cloud networks, Security, Storage, encryption,Kerberos algorithm.

Introduction:

Many studies have been reported in the development of cloud networking. All of the internet-based activities have been formed based on computer technology. Since thedata transmission tothe cloud networks do not require complex hardware maintenance, so these systems are more compatible with the users.The cloud computing is the model for comprehensive and convenient access that can be provided upon request from shared computing resources, quickly and with minimal management effort or interaction with the service provider (Dahal, 2012). The cloud network has the ability to act as a host forthe distributed services andapplications (Hamze et al, 2014). In fact, the cloud computing is providing a new platform for sharing successful data transmission on the Web service (Yildirim and Girici, 2014). Similar to other data transmission networks, cloud networks are also has problems.

The security and users privacy are the major problem ofthe cloud network. Nowadays, due to over increasing volume of data storage andcomputational methods variation in these networks, the responsibility of local tools to maintain the existing data are declining. Thus, in the long term, the data security and privacy that always are considered as one of the most important aspects of service quality create a major challenge for the cloud networks. Other challenges facing the cloud networks are multiple updatesof the information stored on these networks. Activates that performed on updatingthe information by users are including:attachment, deletion, modification, adding, sorting, and so on.Therefore, in this case,the cloud network providers also consider the dynamic security. Now, the data centers are responsible for the operation of secureproviding, which simultaneously carry out the collaboration and distribution of data.

According to this, at first the user's data are stored separately in the physical environment, so that the potential threats of the data integrity is reduced and eventually after storage operations, data are transferred to the cloud networks.Hence, it can be concluded that the distributed protocols are considered as the main element in order to ensure the correct data storage in the cloud network of storage systems (Dahal, 2012).

The current encryption systems

Data security are considered as one of the most important aspects of the service quality in the communication networks. The cloud computing is also necessarily requires the use of new security systems (Ascorti et al, 2014). Therefore, the two issues are important:

-In the early stages of data protection,the traditional encryption methods cannot use directly, because it leads to the loss of user control on existence data in the cloud networks. So, the receiving the confirmation of correct data storage in the cloud environment, should be separated from other existing data. This problem is significant from the aspect that the security demands of the various data, whichstored in the cloud environment, will be challenging in the long term.

-Cloud network storage are used only as a third party to store the data. The stored data by the user in these environments are constantly changing, evolving and updating (operations such as attachment, deletion, modification, addition, reordering etc.), thus ensuring correct data storage has a great importance due to the dynamic operations.

Although in the mentioned methods in the field ofstorage of processed data accuracy, users do not need to have access,these methods cannot cover all available security threats in the cloud network of data storage. In fact, the reason for the methods weakness is their focus on only one-server functions and not considering of dynamic data operations. Therefore, the researchers in order to increase the confidence in data storage security have used a complementary approach.

This is the way from the distributed protocols across multiple separate servers. In addition, the new method uses asymmetric and symmetric encryption systems in the field of data storage security and other methods used triple encryption method, RSA, elliptic curves and advanced encryption. The important point related with the use of distributed protocols and encryption algorithms is that, firstly, the distributed protocols do not have any knowledge about the functions of dynamic data, and secondly, using the encryption algorithms reduces the system performance. As a result, the application of mentioned methods in the accuracy assessment of cloud storage environment is dramatically reducing.

The proposed algorithm

Due to the difficulties in applying the current encryption methods and distributed protocols, we investigated the effects Kerberos algorithms in cloud computing servers in this study. The Kerberos algorithm used to enhance the security level of data storage accuracy in the cloud network. A strong encryption model and a ticket-granting algorithm used in order to authenticate the users of the network. According to this algorithm, all users need to present the IP and password for the updating operations. So all users must pre-register by Kerberosalgorithms in the cloud. The following figure indicates the user's login operation.

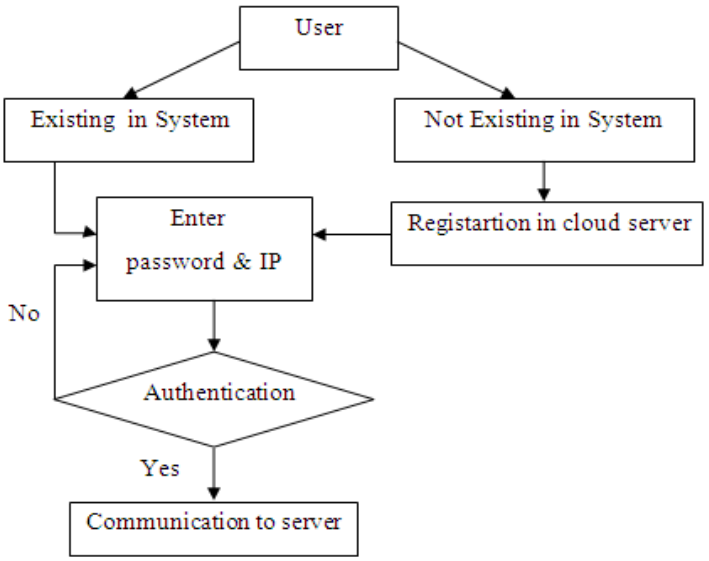


Figure 1: Users login operation to enter the server

According to the mentioned points about the Kerberos algorithm in this study, we have proposed an effective distribution plan with a clear support model for dynamic data systems.

The proposed structure significantly reduces the communication and data storage operations compared with the replication-based file distribution methods. In addition, this model could reach to its goal, which is ensuring the correct storage and errors localization by usingsimilar signs and confirmation of distributed data via the safe code.In fact, anywhere that data corruption is detected;our model can guaranteethe simultaneous localization operations of the data error, which leads to identify misbehaving servers. The following figure represents the cloud environment structure and data security of a cloud server.

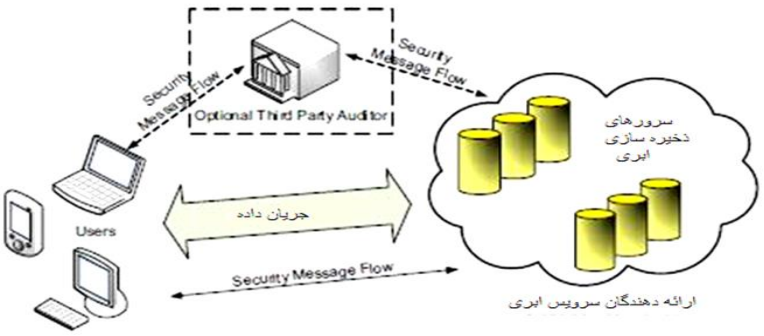


Figure 2: structure of cloud computing system

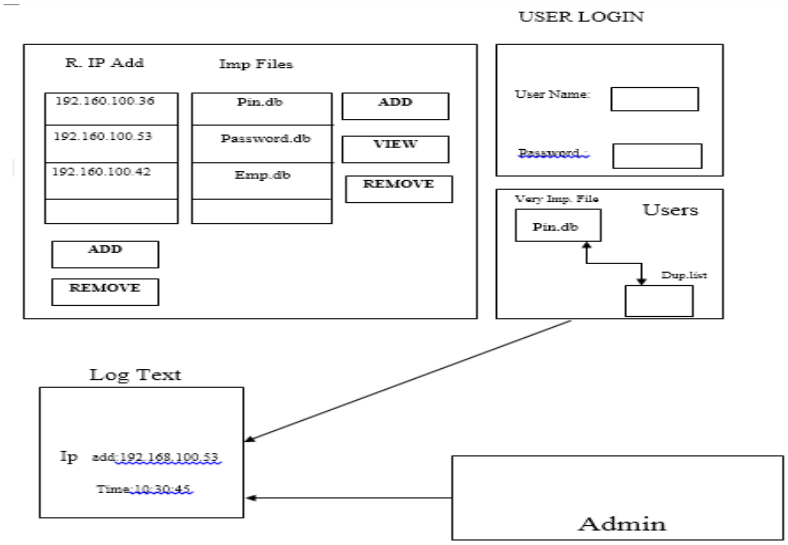


Figure 3: structure of data security of a cloud server

As already stated, the most important operations in the cloud network are storage method and users authentication by servers in the cloud servers. We describes the operation as follows:

Data storage module

In order to perform a save operation, through a CSP, the user saves data in a set of cloud servers so that the servers run at the same time. In this case,through the same CSP, the user interacts with the cloud environment to have access to the data. In some cases, the user may need an operation on his block-level data. In this case, users need to correct stored data, which are equipped with security devices. Based on the proposed model in this study, we have assumed that there are communication channels, whichlocated between servers in the cloud as a point-to-point, and all of the users on the network are reliable. Consequently, because of these two important factors in the proposed model, the data storage is performed with higher speed and safety.

Cloud server authentication

The cloud server performance in authentication is like the other authentication systems. Therefore, in the proposed system, by adding only some extra features to the custom user authentication protocols, it is possible tomanage the logging operation of cloud. The authentication system acts in such a way that immediately after sending information from the user to the router, the system is changed. In this model, the authentication system acts as a ticket and is a controller of application licenses. This systemreduced the user authentication time and deletion, due to the update operation support for the clients.

System test results

One of the main features of successful software products, in the long time,is the success of various tests at the time of manufacture or later on the application. If the number of tests is more and the error rate is lower, it can be ensured that the system or model has the good ability. Our production system have verified through the tests such as integration testing, functional, white box, black box, system and unit test. Based on the experiments have been done on the system, it was revealed that:

- All entries have been signed with a correct format.
- Duplicate entry are not allowed to enter the system.
- All communication lines of the systems function properly and guide the user to a requested page.

Finally,it can be noted that the system has successfully passed all the tests and without any fault carried out its activities.

Conclusion:

The aim of this study was to achieve a model to ensure aboutthe correctness of stored data updating operation in the cloud. The flexible and efficient model based on the Kerberos algorithm was proposed which is able to dynamically support the update operation. We could propose theintegrated plan to ensure correct storage using similar signs and confirmed distribution of data without the code. In comparison to many previous methods that only binary results of distributed servers offer storage scenarios, challenge/response protocol presented in this study can localize data errors. In addition,another advantage of this researchis its support ofdynamic and efficient functions to the integrity of the data.Finally, based on the exact analysis in the security cloud network and performed various tests on the produced systems, we notice that the proposed model is efficient and resistant against the Byzantine fault tolerance, malware attacks and even collusion attack servers.

References:

Ascorti, L., Savazzi, S., & Galimberti, S. (2014). Cloud-based wirelesshart networking for critical industrial monitoring and control. Paper presented at the 12th IEEE International Conference on Industrial Informatics (INDIN), Porto Alegre, PP. 362 - 369.

Dahal, S. (2012). Security Architecture for Cloud Computing Platform. (Master of Thesis), Stockholm University, Sweden.

Hamze, M., Mbarek, N., & Togni, O. (2014). Autonomic Brokerage Service for an End-to-End Cloud Networking Service Level Agreement.Paper presented at the 3rd Symposium on Network Cloud Computing and Applications (NCCA), Rome,PP.54 -61.

Hassan, S. A. Z. (2013). SONA: A service oriented nodes architecture for developing Cloud Computing applications. Paper presented at the International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore,PP.1-6.

Halvachy, H (1392). A secure architecture for privacy, confidentiality, and data integrity. (MSc), Sharif University of Technology.

Idris, A. S., Anuar, N., Mokhsin, M., & Fauzi, F. H. M. (2014). The readiness of Cloud Computing: A case study in Politeknik Sultan Salahuddin Abdul Aziz Shah, Shah Alam. Paper presented at the International Conference on Computational Science andTechnology (ICCST), Kota Kinabalu, PP.1-5.

Lawey, A. Q., El-Gorashi, T. E. H., & Elmirghani, J. M. H. (2014). Distributed Energy Efficient Clouds Over Core Networks. Journal of Lightwave Technology,Vol.32,No.7, PP. 1261 - 1281.

Naghyan Fesharaki, M; Tabatabaei, S.Gh.H. and Tamtajy, D. (1393) Private cloud computing reference architecture providing perimeter security agencies. Journal of "security studies", S.91-113.

Omar, M. N., Salleh, M., & Bakhtiari, M. (2014). Biometric encryption to enhance confidentiality in Cloud computin. Paper presented at the International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, PP.45-50.

Taravat, A., Frate, F. D., Cornaro, C., & Vergari, S. (2015). Neural Networks and Support Vector Machine Algorithms for Automatic Cloud Classification of Whole-Sky Ground-Based Images Geoscience and Remote Sensing Letters, Vol.12, No.3, PP. 666 - 670

Velasco, L., Contreras, L. M., Ferraris, G., Stavdas, A., Cugini, F., Wiegand, M., & Fernández-Palacios, J. P. (2015). A Service-Oriented Hybrid Access Network and Clouds Architecture. Communications Magazine, Vol.53No.4, PP.159 - 165

Wang, X. (2015). IPv6-based vehicular cloud networking. Communications Letters, Vol.19,No.6, PP. 933 – 936.

Yildirim, A. S., & Girici, T. (2014). Cloud Technology and Performance Improvement With Intserv over Diffserv for Cloud Computing. Paper presented at the International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, PP.222-229.