Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 52 (2015) 1153 – 1158

Procedia Computer Science

First International Workshop on Mobile Cloud Computing Systems, Management, and Security (MCSMS-2015)

A Secure Cloud Computing Model based on Data Classification

Lo'ai Tawalbeh[1,*], Nour S. Darwazeh[2], Raad S. Al-Qassas[2] and Fahd AlDosari[1]

[1]*Computer Engineering Department, Umm-Alqura University, Makkah, Saudi Arabia,*
Email: latawalbeh@uqu.edu.sa, fmdosari@uqu.edu.sa.
[2] *Department of Computer Science, Princess Sumaya University for Technology, Amman, Jordan.*
ndrwazeh@gmail.com, raad@psut.edu.jo

Abstract

In cloud computing systems, the data is stored on remote servers accessed through the internet. The increasing volume of personal and vital data, brings up more focus on storing the data securely. Data can include financial transactions, important documents, and multimedia contents. Implementing cloud computing services may reduce local storage reliance in addition to reducing operational and maintenance costs. However, users still have major security and privacy concerns about their outsourced data because of possible unauthorized access within the service providers. The existing solutions encrypt all data using the same key size without taking into consideration the confidentiality level of data which in turn will increase the cost and processing time. In this research, we propose a secure cloud computing model based on data classification. The proposed cloud model minimizes the overhead and processing time needed to secure data through using different security mechanisms with variable key sizes to provide the appropriate confidentiality level required for the data. The proposed model was tested with different encryption algorithms, and the simulation results showed the reliability and efficiency of the proposed framework.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Mobile Cloud Computing; Data Security; Cloud Storage; Client Side Encryption; Cryptography

* Corresponding author. Tel.: +966 55 350 6982; Fax: +966 2528 1376
E-mail address: Latawalbeh@uqu.edu.sa

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2015.05.150

1. Introduction

Nowadays, cloud computing is a growing area that involves wide range of new technologies and applications that touches almost every house residents. Among the associated concepts with this area is the Mobile Cloud Computing (MCC) which is basically allows the users to access and use the cloud services and applications via mobile devices. But and as we know, the Mobile devices have number of challenges that limit their performance, such as battery life time, and lack of computing resources and storage. Another important issue in Cloud and Mobile Cloud Computing is the security of the stored data.

Cloud storage services are used widely to store and automatically back up arbitrary data in ways that are considered cost saving, easy to use and accessible[1]. They also facilitate data sharing between users and synchronization of multiple devices. But, there are vital data that is processed and stored in the cloud systems. Losing or exposing these valuable data will have huge bad impact on the data owners being individuals or organizations. And so, there is an increasing demand to protect data over the cloud systems.

Users fear from uploading private and confidential files to the online backup due to concerns that the service provider might use them inappropriately. Adding to that, there are concerns about their data being hacked and compromised due to the spread of cloud storage successful attacks [2].

The existing cloud storage frameworks use same key size to encrypt all data without taking in consideration its confidentiality level which might be infeasible. Treating the low and high confidential data by the same way and at the same security level will add unnecessary overhead and increase the processing time.

Motivated by the above facts, this paper focuses on two important aspects of mobile computing, security and storage. The confidentiality of data is very important in cloud environment, and based on that, we propose an efficient framework that provide data confidentiality and integrity in cloud storage in both transmission and storing operations. Moreover, this framework will reduces the complexity and processing time used to encrypt the data.

The rest of this paper is organized as follows: Section two shows related literature review. In Section three, we propose our secure cloud framework that will be simulated for performance evaluation in section four. Finally, section six concludes this work.

2. Related Work and Existing Solutions

Cloud storage provides users with great benefits and advantages. It provides better accessibility, for instance it enables them to access data from any device connected to the internet. There is no need for users to bring their physical storage devices wherever they are and they can use any computer for saving and retrieving their information. It enhances teamwork and collaborative efforts by allowing team members to access shared data. In addition to that, cloud storage is cost saving due to not having to buy or maintain expensive hardware. Also, it can be used for backup, archival and disaster recovery purposes. Moreover, the data are stored on many servers to guarantee a sustainable service to the clients so that they are able to access their data at any time[8,9,10].

Despite all the benefits a user can get from cloud storage services, it still has its limitations. When speaking about public cloud storage, data is no longer in the hands of the user, it is actually stored on remote servers, and it is mostly spread around the globe. Deleting one file does not guarantee you that it has been truly deleted [11,12].

The number of cloud storage providers on the internet seems to be increasing rapidly, Examples of cloud storage providers are Google Docs, Dropbox, JustCloud, Mozy and Google Drive are all examples of services that provide storage space for digital data.

Standalone software can encrypt all the data on the user system, however this has some disadvantages. The standalone software is installed, controlled and ran on both the client side and the cloud storage provider side. All devices that have access to the stored data should know the key used in encrypting it. In case the key was lost, decrypting data will never be possible again. To prevent data loss, keys used for encrypting data must be combined into some kind of a key escrow system. Generation of keys used for encrypting data must be truly random which will guarantee difference in two ciphers of the same clear text [10,12].

Another important area that is growing fast these days is the Mobile Cloud Computing (MCC). This area includes acceding the cloud services via mobile devices. And as we know, these mobile devices has limited capabilities that include limited power and storage. So providing an efficient secure storage framework is very

helpful in mobile cloud computing area. The work in[13] focuses mainly on how to use mobile cloud computing for data collection in large scale networks. The authors in[14] provide a Scalable Cloudlet-based Mobile Computing Model, and followed by extension to build a large scale deployment of cloudlets using the CloudExp tool [15].

SecCSIE: A secure cloud storage integrator for enterprises: Seiger et al.[5] proposed a flexible system architecture named SecCSIE to combine various types of cloud storage providers to the employee's computer with ensuring data security. The architecture proposed is versatile, and centralized around a proxy server which will encrypt all the outsourced files and apply information dispersion to them before leaving the internal network. Moreover, it ensures data confidentiality, integrity and availability. The main objective of this architecture is to extend the internal IT resources of the organization by a very accessible and enduring external storage services like the present cloud computing service providers. They are concerned with attaining the highest level of security besides excellent usability and extensibility.

DEPSKY: dependable and secure storage in a cloud-of-clouds: Bessani et al.[3] proposed DEPSKY a secure and reliable system that takes a responsibility in improving the availability, integrity and confidentiality of the stored information by encrypting, encoding and replicating data on different clouds that form a cloud-of-clouds. The system was implemented using four cloud storage service providers (Amazon S3, Windows Azure, Nirvanix and Rackspace) and PlanetLab to run clients that access the service from numerous places around the world. The paper outlines four drawbacks of the individual cloud 1) Loss of availability 2) Loss and corruption of data 3) Loss of privacy 4) Vendor lock-in. It describes how the DEPSKY system succeed in dealing with them by using an effective set of Byzantine quorum system protocols, cryptography, secret sharing, erasure codes and the variety which comes from using more than a single cloud.

CloudSafe: Storing Your Digital Asset in the Cloud-based Safe: Zhang et al.[7] proposed CloudSafe to enhance availability and confidentiality of the stored information in the cloud through encrypting and encoding data into several cloud storage providers. In order to make a safe, dependable and quick data access repository possible, CloudSafe offers a cloud-based personal digital asset safe service which delivers the valuable assets between several cloud providers by using erasure coding and cryptography. The storage providers are: Dropbox, Google Drive, Microsoft SkyDrive and SugarSync. According to Zhang et al., the availability improves due to using erasure coding to distribute the data on several cloud providers, in order to recover data access when a provider fails. AES[24] have been used for encrypting and decrypting data to keep data confidentiality.

A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding: Lin et al.[4] proposed a threshold proxy re-encryption scheme and combined it with a non-centralized erasure code to design a secure distributed storage system that offers secure and strong data storage and recovery. In addition, the formulated storage system allows users to forward their data to the server and to other users. The proposed system provides strong confidentiality and secrecy of messages in storage servers. The re-encryption scheme boosts encoding operations over encrypted messages and forwarding operations over encoded and encrypted messages. But each of these solutions has many limitations. Seiger et al.[5] has a few limitations like that it needs more management and resources, keys are managed by the provider and data is exposed to hacking attacks when a user sends it to the servers of the service provider or in case the hacker breaks the transmission security protocol. Bessani et al.[9] requires a lot of physical resources thus increases costs. Another limitation of the paper is that keys could be managed by many servers which will increase risk. Somani et al. [6] also has a few limitations for example it uses the RSA encryption technique that is less secure and slow in encrypting and decrypting large amount of data. RSA contains a public and a private key therefore the solution needs key management from a third party, which will increase risk.

3. The Proposed secure cloud computing model based on data classification

In this paper, our target is to handle two issues the user encounter when using cloud computing services. The first one is users concerns about hacking threats whether internally or externally. The other one is the infeasibility of encrypting all data without taking into consideration its confidentiality degree. Therefore, we propose a framework that allows the users to encrypt own data using a key that is not available for the provider. In addition we encrypt data bases on the degree of confidentiality.

For example it's not feasible to encrypt a 100GB data block entirely using the same key size and security level because it could only contain 20% of confidential data. In other words, it would be a waste of time because of the very high processing time it takes to encrypt data entirely using the same security level and key size. Taking into consideration the degree of confidentiality in classifying data would save time and encrypt the less important data with a basic level of security instead of a highly confidential one.

Therefore, we propose our secure cloud storage model that encrypts data according to its confidentiality degree through three levels: basic, confidential and highly confidential. The proposed solution is based on the idea of manual classification, which means that the user will specify the confidentiality level of data.

In the sequel of this section we will present our proposed framework in detail. We also explain briefly the data classification process and illustrate the work of well-known encryption and cryptographic algorithms like AES, TLS and SHA which are used to ensure confidentiality and integrity of data. In addition to discussing the survey that we have conducted to help us in building our framework.

Data classification[19] is the process that allows organizations and individuals to categorize all different kinds of data and information assets according to its confidentiality degree, which will determine the extent of security the data needs. Classification is made to guarantee information sensitivity and an appropriate protection for the by-low protected information. Data can also be categorized in accordance to how frequently it must be accessed i.e. to its critical value. Data with higher critical value will be stored on a faster media whereas data that are less critical are stored on slower media. Different encryption algorithms and cryptographic functions such as Secure Hashing Algorithm (SHA)[16], Advanced Encryption Standard (AES)[17] and Transport Layer Security (TLS)[19] are used based on the security level of the data.

3.1. *Framework details*

The three security levels in the proposed model are shown in Figure 1: basic, confidential and highly confidential.

- Basic level**:** The basic level is concerned in encrypting a general type of data like, videos and photos that do not need a high degree of confidentiality. Hence, this level offers a basic level of security and is used by most of the products available online. For that, we recommend using TLS for encrypting the communication between the application of the client and the server using HTTPS. TLS guarantees communication privacy between users on the internet. In addition to the TLS, we recommend using AES-256 for encrypting the data stored on cloud storage servers. It is important to note that data in the basic level of security will not be encrypted at the client side; it will be encrypted using the encryption key of the backup service after transferring the data on the server side. Many storage service providers use TLS and AES-256 such as Mozy and Dropbox.
- Confidential level**:** Confidential level is designed for data with medium confidentiality degree like personal files, photos and videos. In this level, the encryption is done at the client side i.e. it is based on client side encryption. At the confidential level we use AES. The symmetric-key block encrypting algorithm with a fixed block size of 128-bits and a key length of 128. The mathematical operations in AES are done in 10 rounds for 128-bit keys. Each round consists of multiple processing steps we explained earlier in this section.
- Highly confidential level: This level handles the most important data such as financial transactions and military information. Users are very concerned about losing this type of data and still avoid using all the new offered services because of the high confidentiality of the data and the doubts he may have. Therefore, at this level of security the user is provided with a very high degree of confidentiality and integrity by using two recommended algorithms. The first one is the AES-256 encryption algorithm, which is also recommended by the U.S. National Security Agency (NSA) for encrypting top-secret data in order to prevent unauthorized access. The second one is the secure hashing algorithm SHA-2.

  The algorithm assures integrity of the data. It is performed on the data before sending or uploading it by calculating a hash value. When the user retrieves the data back, the algorithm calculates the hash value for retrieved data, if the value is the same as the first one then the user can be sure that the data was not tampered.

4. Performance evaluation

We have built a simulator to evaluate the proposed framework. The simulator was developed using Microsoft .Net C# with the support of library System Security which is implemented within C# and using the default settings in Microsoft .NET Framework 4.5. We have done all necessary validations and verifications. All simulation experiments were conducted using the same platform: Intel(R) Core(TM) i7-2600K CPU, processor speed 3.40GHz, and RAM of 3 GB. The operating system is Microsoft Windows NT 6.1.7601 SP1. We used the provided classes in Microsoft .Net environment to simulate 3DES, AES128 and AES256. Security library that provides the functionality of a cryptographic cipher used for encryption and decryption.

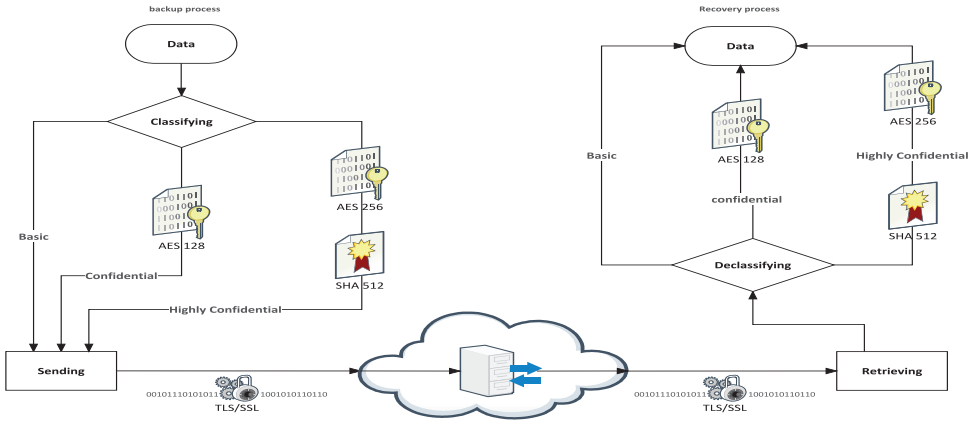

Fig. 1. The proposed secure cloud framework

We have tested the performance of symmetric algorithms including AES128, AES256 and 3DES. The performance evaluation is based on the time needed to encrypt data blocks with different sizes varied between 2 GB and 10 GB. The results showed that AES128 has outperformed the other algorithms in terms of speed in encrypting data blocks as it has the lowest processing time compared to other algorithms.

The framework performance evaluation conducted by comparing it against the AES128 as minimum encryption method and against both AES256 and 3DES to guarantee integrity and a relatively high encryption. The experiments were conducted on data blocks with varied sizes.
Figure 2 shows the performance of our framework against that of AES128 and AES256 + SHA2, when

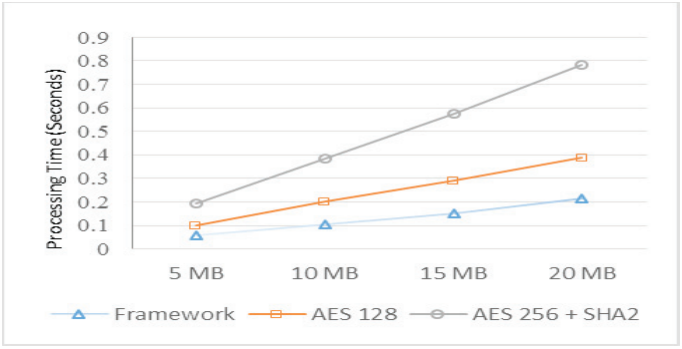

Fig. 2. Performance Evaluation of the proposed framework

encrypting small data blocks ranging from 5 MB to 20 MB. The x-axis represents the sizes of the data blocks in megabytes and the y-axis represents the processing time in seconds. Our framework clearly outperforms the other solutions, and this is because the other solutions encrypt all data regardless of the required confidentiality level.

5. Conclusions

In this paper, we have proposed an efficient confidentiality-based cloud storage framework that enhances the processing time and assures confidentiality and integrity through data classification and applying TLS, AES and SHA based on the type of classified data. The efficiency of our proposed framework has been shown through conducting simulations. The simulation results show that our framework achieves better processing time while assuring data confidentiality and integrity. As part of our future work, we plan to enhance our framework by considering other aspects. This includes automatic data classification and the use of different cryptographic algorithms such as asymmetric public key, RSA, and Elliptic curve cryptography that could provide higher degree of confidentiality and security.

Acknowledgment

The authors would like to thank Deanship of Scientific Research at Umm Al-Qura University (project # 43408022) for the financial support.

References

1. Wu J, Ping L, Ge X, Wang Y, Fu J. Cloud Storage as the Infrastructure of Cloud Computing. International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), 22-23 June 2010; 380-383.
2. Ogigau-Neamtiu F. Cloud Computing Security Issues. Journal of Defense Resources Management 2012; 3(2):141-148.
3. Bessani A, Correia M, Quaresma B, Andre F, Sousa P. DepSky: dependable and secure storage in a cloud-of-clouds. Proceedings of the sixth conference on Computer systems, April 2011; 31-46.
4. Lin H-Y, Tzeng WG. A secure erasure code-based cloud storage system with secure data forwarding. Parallel and Distributed Systems, IEEE Transactions on 2012; 23(6):995-1003.
5. Seiger R, Groß S, Schill A. SecCSIE: a secure cloud storage integrator for enterprises. IEEE 13th Conference on Commerce and Enterprise Computing (CEC); 252-255.
6. Somani U, Lakhani K, Mundra M. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. International Conference on Parallel Distributed and Grid Computing (PDGC); 211-216.
7. Zhang Q, Luo B, Shi W, Almoharib AM. 2013. CloudSafe: Storing Your Digital Asset in the Cloud-based Safe. Wayne State University.
8. Brindha T, Shaji RS, Rajesh GP. A Survey on the Architectures of Data Security in Cloud Storage Infrastructure. International Journal of Engineering & Technology 2013; 5(2):1108-1114.
9. Kamara S, Lauter K. Cryptographic cloud storage. Financial Cryptography and Data Security. Springer; 2010; 136-149.
10. Wei Y, Jianpeng Z, Junmao Z, Wei Z, Xinlei Y. Design and Implementation of Security Cloud Storage Framework. Proceedings of the 2nd International Conference on Instrumentation, Measurement, Computer, Communication and Control, December 2012; 323-326.
11. Borgmann M, Hahn T, Herfert M, Kunz T, Richter M, Viebeg U, Vowe S. 2012. On the Security of Cloud Storage Services. Fraunhofer Institute for Secure Information Technology SIT.
12. Jararweh, Yaser, Ola Al-Sharqawi, Nawaf Abdulla, Lo'ai Tawalbeh, and Mohammad Alhammouri. "High-Throughput Encryption for Cloud Computing Storage System." International Journal of Cloud Applications and Computing (IJCAC) 4, no. 2 (2014): 1-14.
13. Jararweh, Y.; Tawalbeh, L.; Ababneh, F.; Dosari, F., "Resource Efficient Mobile Computing Using Cloudlet Infrastructure," 2013 IEEE Ninth International Conference on Mobile Ad-hoc and Sensor Networks (MSN), , vol., no., pp.373,377, 11-13 Dec. 2013
14. Yaser. Jararweh, Lo'ai Tawalbeh, Fadi Ababneh, Abdallah Khreishah, Fahd Dosari, Scalable Cloudlet-based Mobile Computing Model, Procedia Computer Science, Volume 34, 2014, Pages 434-441, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2014.07.051.
15. Lo'ai Tawalbeh, Yaser Jararweh, Fadi ababneh and Fahd Dosari. Large Scale Cloudlets Deployment for Efficent Mobile Cloud Computing. Journal of Networks. Vol 10, No 01 (2015), 70-76, Feb 2015
16. Secure Hash Standard (SHS), FIPS PUB 180-4. National Institute of Standards and Technology 2012.
17. Moh'd, Abidalrahman, Yaser Jararweh, and L. Tawalbeh. "AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation." In Information Assurance and Security (IAS), 2011 7th International Conference on, pp. 292-297. IEEE, 2011.
18. Ko RKL, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, Lee BS. TrustCloud: A framework for accountability and trust in cloud computing. IEEE World Congress on Services (SERVICES); 584-588.
19. Freier A, Karlton P, Kocher P. The Secure Sockets Layer (SSL) Protocol V. 3.0, RFC 6101. Internet Engineering Task Force (IETF) 2011.