International Journal of Engineering & Technology, 7 (4.15) (2018) 98-102

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Mobile Application Design for Protecting the Data in Cloud Using Enhanced Technique of Encryption

Sakinah Ali Pitchay[1,2]*, Wail Abdo Ali Alhiagem[1], Farida Ridzuan[1,2], Sundresan Perumal[1]

[1]Faculty of Science and Technology,
[2]CyberSecurity and Systems Research Unit, Islamic Science Institute (ISI),
Universiti Sains Islam Malaysia (USIM), Negeri Sembilan, Malaysia
**Corresponding author E-mail: sakinah.ali@usim.edu.my*

Abstract

This paper provides an enhanced technique for improving the security and protecting the privacy of the cloud computing users by encrypting the data before it reached to server's storage. Encrypting means the process of converting information or data into unreadable language to prevent unauthorized access. This paper will propose a mobile application design, which will allow the user to encrypt and decrypt the data hence maintaining security and privacy. In the proposed system design, the AES Algorithm will handle the encryption of the data using a keyword which will be defined by the user during the creation of the account. The encryption keyword will be hashed by the system using MD5 Algorithm. The keys will remain in encrypted form, while they are on the server side. Both encrypted data, encryption and decryption keys will be saved on the server in secured form. The idea behind hashing the encryption keys is to protect the keys while they are stored on the server, therefore, any unauthorized access to the server will gain no advantages since every bit of data on the server is encrypted including the private keys. The proposed system design will participate by improving the security and privacy of the users by giving them the capability to encrypt and decrypt data in enhanced way using AES as a data encryption method and MD5 hash algorithm for encrypting the encryption keys.

Keywords: *Big Data Security; Cloud Computing; Encryption; MD5 Hashing.*

1. Introduction

Cloud computing can be defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Mobile phones are one of the most widely used technological equipment which used by billions. The evolution of mobile phones has even gotten faster with the invention of the internet communication protocol which allowed far remote connections. Cloud computing is also known as the use of computing resources which are delivered to the users as a service over a network. With the current services provided by cloud computing providers it has become easy for the end users use the service and store their data in online servers. With the feature mentioned of cloud computing, end users must pay attention to the security and privacy side since the providers never guarantee the security of the data or provide service-level agreement (SLA) [1].

The remainder of the paper is organized as follows. Section 2 highlights the security issues in cloud computing and Section 3 investigates the existing solutions for security issues. Section 4 proposes the design concept architecture. In Section 5, use case diagram is designed. In section 6, system design workflow is presented and Section 7 summarizes the expected result. Finally, Section 8 concludes the paper.

2. Issues in Cloud Computing

In the recent years of internet computing, the rising reputation of cloud computing has attracted a large amount of internet users. Besides individual users, many groups, organizations, and big companies do benefit from cloud computing services due the valued services provided, which allows permanent online storage of important data. The problem blooms then where end users and companies store their highly confidential data in cloud computing servers with no guarantee of data protection [2-4]. In fact, cloud computing servers are highly protected against hacking, but the data is still accessible by unauthorized people in the server maintenance tasks.

According to [5], most distributed systems computations have only a single level of protection, which is not recommended and automated data transfer requires additional security measures, which are often not available. Moreover, unethical IT specialists practicing information mining can gather personal data without asking users for permission or notifying them. These three issues are also have been identified in the Big Data security challenges. In this section the privacy issues, security, and access control will be discussed and highlighted.

2.1. Security Issues

There are numerous security issues in cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

management, load balancing, concurrency control and memory management [6-7]. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud must be secured. When users upload their data to cloud servers, it becomes possible for the data to be accessed by anyhow, whether by the maintenance team or by hackers. Cloud computing providers never guarantee the protection of the data, so the only best way to cover this issue is to have the data encrypted before it reaches the cloud servers.

2.2. Privacy Issues

The main concern around data privacy is the protection of information from unauthorized access [8]. One of the most important goals needs to be achieved in cloud computing security is protecting data privacy. It is difficult to prevent threats in cloud computing because it is a shared environment that depend on a shared infrastructure. Therefore, information will be exposed to the risk of unauthorized access. In other word, we face a big challenge when we talk about sharing a cloud computing resources to protecting customer privacy. The important step to solve this challenge is encrypting the data before it reaches to cloud servers [9].

2.3. Access Control

Access control can be defined as a security technique that can be used to regulate who or what can view or use resources in a computing environment. Access control has become more important than ever, since the cloud and all its data are accessible to anyone over the Internet [7]. One of many issues of the cloud computing is access control. Access control means that the value of data that we have at local or online storage must be protected from accessing or editing, so the best solution for this issue it to keep the data encrypted at all time and implement a new method for accessing the data.

As a conclusion to the discussed points, there is a requirement of assuring that the data stored on the server is only accessible by the owner. Privacy and security of the data are the main important factors which need to look at since the data is stored in online servers where it can be accessed by authorized people, whether by the hackers or by the maintenance team at the server side [3].

3. Existing Solutions for Security Issues

Cloud computing is suffering from a number of known vulnerabilities, which enable attackers to steal information from cloud users. In the world of computing, security, privacy and access control issues are a major concern of cloud computing [10-11]. There are many studies have been conducted to improve the security and protect the privacy of user's data at the cloud servers. According to [12], the security and privacy issues have been discussed and they proposed a new technique for protecting the data of the users by implementing the encryption and decryption methods using AES and RSA encryption algorithm. The idea which was proposed by them is working based on data partition, which means that the data will be partitioned then it will be encrypted before it is sent to the server using AES and RSA. After the encryption process, the partitioned data will be sent to several servers. When users wish to get back their data, the partitioned data will be downloaded and they decrypt it back using the same method.

A study by [12] has proposed a new way of protecting the data at cloud storage. The proposed method of this study mainly focused on encrypting the data using RSA encryption algorithm. The reason of using the RSA algorithm is to secure the data and improve the security and privacy at the cloud. In this study the original data will be encrypted using RSA algorithm, during the encryption process RSA will generate Private keys which are used for encryption and decryption. Those keys are uploaded with the original encrypted files. The use of MD5 is to verify the contents of the private keys which are uploaded to the servers.

A paper by [13] has suggested a new technique for improving the integrity of the data at the cloud storage. The paper has proposed RSA algorithm for secured communication, AES for Secured file encryption, MD5 hashing algorithm for hashing the one-time password, and one-time password for authentication. In this study AES Algorithm was proposed to encrypt the original file before the uploading the data to the cloud. The key is kept in the database table of the system server along with the user account name. Before inserting the user account name, it is also hashed using MD5 hashing. This insures that unauthorized person cannot retrieve the key to decrypt a file for a user by simply gaining access and observing the database table of the system server. As a result, the key for a file becomes hidden and safe.

Another study for improving the security of the data done by [14]. The proposed method for securing the data and protecting user's privacy in this study is an advanced method since the encryption and decryption method proposed is based on a combination of AES and RSA encryption algorithm. In this study, the AES has been assigned for files encryption and the RSA encryption algorithm is assigned for keys encryption, which means that the original data which need to be encrypted will be handled by AES, then the process of encrypting the keys which are used for encryption and decryption will be handled by the RSA meaning that there will be two values at the server which are the encrypted files and the encryption and decryption keys, both of the values will be saved at the server in encrypted form.

As a conclusion to the reviewed studies, encryption technique is one of the most effective methods to secure the data at the cloud storage since it transfers every bit of data to unreadable language. The investigated studies focused on using the AES, RSA and MD5 encryption algorithm to enhance the security of the cloud storage by applying the encryption technology to the data before the transmission process to online servers. MD5 was proposed to hide the information using images during the transmission of the data and while the data is remained at the server.

In the proposed system design, the AES encryption algorithm will be employed for encrypting the original data, while the use of MD5 will be used for hashing the private keys, which will encrypt and decrypt the data. The idea behind hashing the encryption keys is to protect the keys while they are stored at the server, therefore, any unauthorized access to the server will gain no advantages since every bit of data in the sever is encrypted including the private keys.

4. Proposed System Design Concept

The proposed system does not intend to create a new encryption algorithm or cloud computing implementation. This proposed system recommends a new method on how the data is encrypted in the cloud by suggesting a new way of encryption and decryption using advance encryption standard (AES) and message digest algorithm 5 (MD5) [15-17]. The use of the AES will be for encrypting the original data, while the use of the MD5 will be for hashing the encryption keys. Most users are not comfortable by knowing that their extremely private or confidential data can be accessed by hackers or for various purposes by the cloud server providers. This could be for maintenance purposes; security thread claims or even regular file backup processes.

Normally, these reasons are completely valid to protect the cloud server status and performance. However, users are reluctant to upload their confidential data into cloud computing servers without any kind of agreements that give them the advantage to trust. Figure 1 illustrates the overall view of the proposed concept clearly.

The idea behind designing such a system is to overcome the current security and privacy issues of the cloud computing technology. With the current advantages of the internet, such as availability

and speed, it becomes easier for the users to store their valuable data on the cloud servers with just a simple click, but users are still aware of this service due to the breaches in the security and privacy. The proposed system concept is focused on the protection of the data in terms of security, privacy and access control.

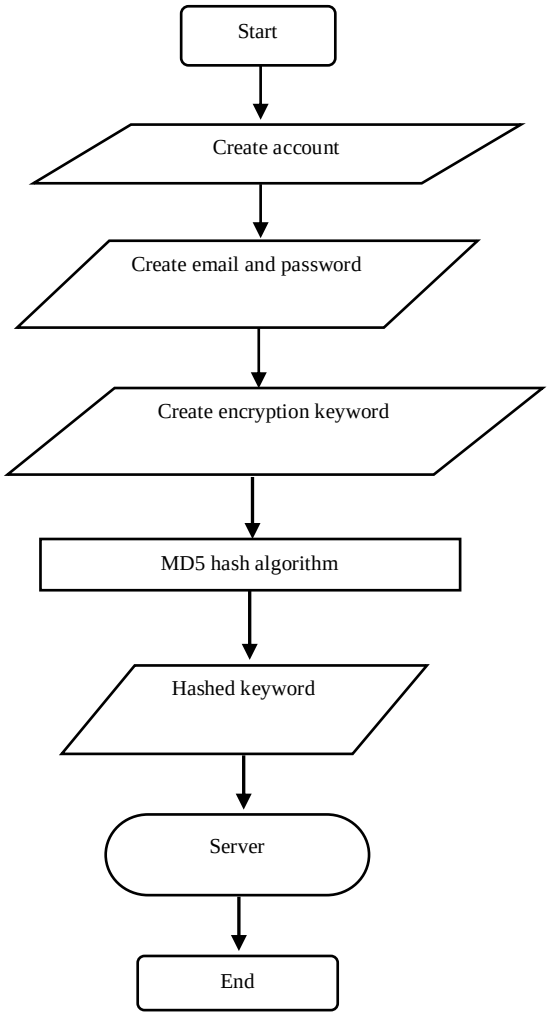


Fig. 1: Overall proposed system design concept architecture using the mobile application.

The best method for securing the data on online servers is to apply encryption before the transmission and uploading process of the data to ensure that the data remain saved and protected in the servers against any authorized access at all time [7, 14]. There are many encryption algorithms in this era, one of the best encryption algorithms is (AES) which stands for advance encryption standard [18]. The overall proposed system structure is for uploading process is shown in Figure 2 and Figure 3 shows the process of downloading. Both processes require encryption and decryption to secure the data.

In the proposed system, the AES Algorithm will handle the encryption of the data using a keyword which will be defined by the user during the creation of the account. The encryption keyword will be hashed by the system using MD5 Algorithm.

5. Design

The proposed system will serve to single type of users. Anyone can easily create an account and use the system to store their data online. Once the account is created, users can upload files with encryption using AES and MD5 algorithm. AES Algorithm will encrypt the original data while the MD5 algorithm will be used for hashing the encryption keys. The upload process will not ask the user for any kind of input. The system will encrypt the data based on the keyword given by the user during the process of the creation of the account. The decryption process and access of the data will require the user to input his keyword for the operation to be accepted. When the user key in his keyword the system will hash the inserted keyword and compare it with the saved hashed key on the server to check if it is the same, if condition applied, then the system will decrypt the data and allow the user to access the data in unencrypted form. The use case diagram for the users' tasks is shown in Figure 4. The major tasks of the proposed system are, uploading with encryption, downloading and accessing the data by a new method and easy technique.

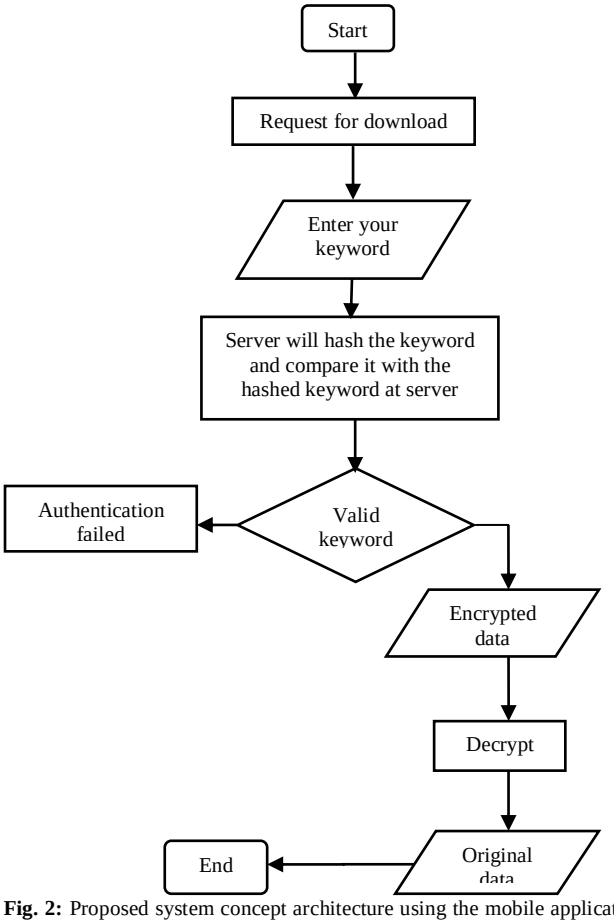


Fig. 2: Proposed system concept architecture using the mobile application for downloading process.

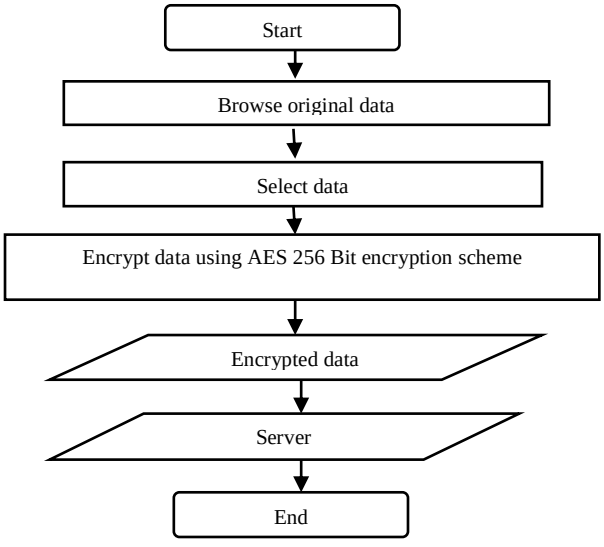


Fig. 3: Proposed system concept architecture using the mobile application for uploading process.

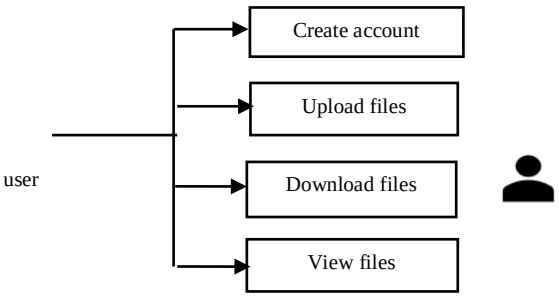


Fig. 4: Use case diagram for the major tasks of the proposed system design.

6. System Work Flow

The designed system will contain three main sections which are the account creation, upload process and download process.

6.1. Account Creation

The account needs to be created for using the system. The user must create an account by filling up his email and password.

6.2. Upload Process

- Login to account.
- Browse data.
- Select files to upload.
- The system will encrypt the data by AES using the encryption keyword which was defined by the user during the account creation.
- The system will upload the encrypted data to the database server.

6.3. Download Process

- Login to account.
- Select files to download.
- Enter the keyword decryption key (the system at this point will hash the decryption keyword and compare it to the hashed key which is saved on the server if the entered keyword is the same, then the system will start to download and decrypt.
- Download request will be denied because of wrong authentication.

7. Expected Result

The only possible way to make sure that the data on the cloud servers is secured by applying encryption before uploading the data to the servers. In the proposed system design, the AES encryption algorithm will be employed for encrypting the original data, while the MD5 will be used for hashing the private keys, which will encrypt and decrypt the data. The idea behind hashing the encryption keys is to protect the encryption keys while they are stored on the server, therefore, any unauthorized access to the server will gain no advantages since every bit of data on the server is encrypted including the private keys. By applying the proposed encryption method, it can be ensured that the data is more secure while it stays at the servers. Accessing the data will be limited only to the owners who have the technique to decrypt as the data was encrypted by them. As a result, the proposed design will participate in improving the security and privacy of the data and protecting user's right by encrypting each bit of the data using a new method since the encryption and decryption process will be handled by the users. Each encrypted bit will be decrypted only by the encryption and decryption keyword of the user. As a conclusion to this section, the user will have the following advantages from the expected proposed design implementation:

- Enhanced mobile application in term of security and privacy
- Protecting user's data by encrypting and decrypting the data using AES and MD5 algorithm
- New methods of storing encryption and decryption keys on the server based on the MD5 hashing algorithm
- Enhanced data access control

8. Conclusion

Cloud computing service is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications, companies and individual users will remain aware of cloud computing technology unless they assure that their data is secure and protected against any unauthorized access. The best way to overcome these issues is by providing the user the advantages and ability to encrypt and decrypt data by themselves. When applying the proposed encryption method, the data will be more secure while it stays at the servers. Accessing the data will be limited only to the owners who have the technique to decrypt as the data was encrypted by them.
As a result, the proposed design will participate in improving the security and privacy of the data and protecting user's right by encrypting each bit of the data using a new method since the encryption and decryption process will be handled by the users. Each encrypted bit will be decrypted only by the decryption keyword of the user. By improving the security and protecting the privacy of the user in the cloud computing era, users will feel safe and confident to use the service for storing their valuable data and the reputation of the cloud service will be improved. With the mobile application design proposed in this paper the security and privacy of the users are improved in a way that make the users feel save toward this technology. It is believed that if the proposed design turned into an implementation it will participate in making the cloud computing storage more secure and suitable for those who have a valuable and important data to be saved online.

Acknowledgement

This work was supported in part by the Ministry of Higher Education (MOHE) Malaysia under research grant: [FRGS/1/2017/ICT04/USIM/02/1]. The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) and MOHE for the support and facilities provided.

References

[1] Taylor, C. (2017). Cloud Computing and Service Level Agreements (SLAs), http://www.datamation.com/cloud-computing/service-level-agreements.html.
[2] Sailaja, K. & Usharani, M. (2015). Cloud computing security issues, challenges and its solutions in financial sectors. International Journal of Advanced Scientific Technologies, Engineering and Management Sciences, 3(1), 190-196.
[3] Yao, G., Li, Y., Lei, L., Wang, H., & Lin, C. (2016). An efficient dynamic provable data possession scheme in cloud storage. In X. Huang, Y. Xiang, & K. C. Li (Eds.), Green, Pervasive, and Cloud Computing. Cham: Springer, pp. 63-81.
[4] Keerthana, G., Prabu, S., & Swarnalatha, P. (2016). An efficient data security in cloud computing using cryptography. International Journal of Advanced Research in Computer Science and Software Engineering, 6(5), 654-660.
[5] Panchenko, A. (2016). Industry perspectives, nine main challenges in big data security, http://www.datacenterknowledge.com/archives/2016/01/19/nine-main-challenges-big-data-security/.
[6] Olalekan, I., & Kayode, A. (2015). Security and reliability issues in the deployment of cloud computing system. Arabian Journal of Business and Management Review, 5(2), 1-8.

[7] Sen, M., & Choudhury, S. S (2017). Security and privacy issues for cloud computing and its challenges. Review of Computer Engineering Studies, 4(2), 62–66.
[8] Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: Issues and current solutions. International Journal of Advanced Computer Science and Applications, 7(4), 485-498.
[9] Pancholi, V. R., & Patel, B. P. (2016). Enhancement of cloud computing security with secure data storage using AES. International Journal for Innovative Research in Science and Technology, 2(9), 18-21.
[10] Wagh, G., Guran, S., Vira, S, Dung, M., & Chaugule, A. (2017). Securing user's data on cloud using AES. International Journal on Recent and Innovation Trends in Computing and Communication, 5(2), 17–20.
[11] Pitchay, S. A., Alhiagem, W. A. A., Ridzuan, F., & Saudi, M. M. (2015). A proposed system concept on enhancing the encryption and decryption method for cloud computing. Proceedings of the IEEE 17th UKSim-AMSS International Conference on Modelling and Simulation, pp. 201-205.
[12] Chauhan, A., & Gupta, J. (2016). Review on encrypt the text by MD5 and RSA in client cloud approach. International Journal of Advance Research, Ideas and Innovations in Technology, 2, 1-7.
[13] Jaglan, V. (2015). Proposing efficient approach to improve integrity checking in cloud data security. International Journal of Recent Research Aspects, 2(3), 125-129.
[14] Kartit, Z., & El Marraki, M. (2015). Applying encryption algorithm to enhance data security in cloud storage. Engineering Letters, 23(4), 1-6.
[15] Jacob, N. M. (2016). Vulnerability of data security using MD5 function in PHP database design. International Journal of Science and Engineering, 1(1), 11-15.
[16] Pandey T. (2016). A secure data transmission over the cloud computing: using salted MD5. International Journal of Innovative Research in Computer and Communication Engineering, 4(2), 1-6.
[17] Nicholas, K., Wilson, C., Kibe, A. (2017). Enhancing trust in cloud computing using MD5 hashing algorithm and RSA encryption standard. International Journal of Scientific and Engineering Research, 8(3), 550-566.
[18] Gul, F, Amin, A, & Ahsraf, S. (2017). Enhancement of cloud computing security with secure data storage using AES. International Journal of Computer Science and Mobile Computing, 6(7), 27-32.