Journal of Harbin Engineering University Vol 44 No. 8
ISSN: 1006-7043 August 2023

Secure Storage Of Handwritten Documents In Cloud

Umadevi T P [1] and Murugan A[2]

[1] Assistant Professor, Department of Computer Science, JBAS College for Women (Autonomous), Chennai, India,

[2]Associate Professor & Head, PG & Research, Department of Computer Science, Dr. Ambedkar Government Arts College (Autonomous) Affiliated to University of Madras, Chennai, India

Abstract -In today's world everything is becoming digitised. Due to all these digital transaction, huge amount of data is being stored. In recent times, handwritten documents are also stored in cloud. One of the most prevalent issues with cloud computing, is the security. When a hand written document is stored, there are chances for it being tampered. In such a scenario, the validity of the document becomes a major issue. This paper proposes a method to safely store the handwritten document in cloud. A novel encryption method is proposed to protect the document while in storage. The proposed method shows a reduction in the execution time, when compared to the traditional encryption algorithm. The proposed system performs experimental analysis of 700 samples of students , which achieves 90% accuracy.

Introduction

Cloud computing offers multiple services and one of the popular being the Storage as a Service (SaaS). Cloud storage is very similar to computer data storage where the digital data is being stored. This storage is being done in logical pools, and the data is said to be "the cloud". For storing the data in a physical storage device might need a number of servers. These servers might be located in multiple locations along the globe. The environment where it is stored might be owned and managed by a third-party hosting company. These storage providers are solely responsible for ensuring that the data are kept safely. The data needs to be available and accessible to the owner of the data. The storage provider should also make sure that the physical environment where it is stored is secure, protected, and running.

In general, the cloud storage can be one of the four types as given below:

(i) Private cloud storage – The data being stored on the company or organization's intranet

(ii) Public cloud storage – The data being stored in a public or in a service provider that is being hosted by a third party like Google cloud, Amazon Web Services etc.

(iii) Hybrid cloud storage – This acts as a combination of private and public cloud

(iv) Community cloud storage – Here, the storage service is offered for a particular community or business

The cloud storage offers a number of benefits like disaster recovery, being able to access the data from anywhere, low cost incurred in storing the data, scalability and less expenditure in maintaining the data storage server etc. Though the benefits sound amazing the cloud storage providers also have certain disadvantages. The limitations of the cloud storage providers include lack of total control, migration of data from one cloud provider to another, the need for internet connection and having a fixed contract thereby creating a stagnation.

One of the main issues in cloud storage providers has been the issue of data security. In the past, there are numerous occurrences where the cloud storage companies being targeted. For instance, in 2014 the cloud storage provider Dropbox leaked its customers' confidential data. This happened due to a security glitch in its systems.

There is a need to implement some security solutions to protect the sensitive data against unauthorized access. The organizations should educate their employees on the risks posed by sharing the information or just storing information in the cloud.

There have been a lot of solutions that were proposed to secure the data in cloud storage.

These data could be text data, digital documents, hand written or any other vital information. One of the most prevalent solutions has been towards using the cryptographic techniques. This paper proposes a method that uses a novel encryption technique to protect the handwritten when stored in the cloud storage. The encryption method proposed here is to convert the handwritten document into binary form. A substitution is performed on the document and is stored in the cloud. A set of rules are used to do this encryption, this method saves the encryption time and reduces the overhead of the system.

Related Work

Data protection answers for the cloud storage security may use policy-based control on the way the data are moved to and from then cloud. There is a need to ensure that only authorized data goes out of the company and at the same time, the data access is restricted to authorized parties only. Hence, any organization can enforce stricter protections policies around any sensitive data.

One of the crucial security threats has been to data confidentiality [1]. The users or the customers may not be able to trust the Cloud Service Providers (CSP) to a full extent. The reason is due to the fact that the data stored in cloud might be confidential and sensitive [2]. The owners might feel reluctant to store the data over cloud due to the fear where the data might get lost or for any unauthorized access to the data [3].

There have been a number of data leakage incidents resulting in a loss. These kind of real time incidents have escalated the concern [4] [5]. Almutairi *et al.* [6] proposed a virtual resource management methodology by using the Role-Based Access Control (RBAC) policy. This reduces the data exposure. Li *et al.* [7] proposed a privacy-conserving and outsourced classification in cloud computing (POCC) framework using various public keys. A scheme is developed by Gao *et al.* in [8] proposed a model to prevent the attack of information disclosure. This was built to defend against the substitution-then comparison (STC) attack.

Srisakthi et al. [9] proposed a secure encryption model that based on discrete transformation. This method saved space and simultaneously reduced the calculation cost to protect user data. Al-Haj *et al.* [10] provided two crypto-based algorithms that provided confidentiality, integrity, and authenticity.

Proposed System

The proposed system is designed to be a light weight technique model which does not use any of the traditional encryption techniques. Mostly all the traditional encryption algorithms incur time for the execution. Thomas Eisenbarth et al. [11] published a detailed survey on the state-of-the-art cryptographic algorithms. These algorithms were compared with lightweight cryptographic algorithms. The comparison was made over the hardware and software used and on the implementations of the symmetric and asymmetric ciphers. These lightweight cryptographic algorithms were similar to traditional encryption algorithms but had less computational complexity. But these kind of encryption algorithms needed more storage space, and time. Hence, it is not an optimal solution to use encryption algorithms in resource constrained devices.

The proposed model follows a processing of the user data in the binary form. All the security measures are carried out over the user's data after converting it into its equivalent binary form.

The process flow of the method is given in figure 1. And the pseudo code for the process is summarized below:

Secure Storage Of Handwritten Documents In Cloud

Algorithm: Multiple Multilevel User Centric Encryption Algorithm

Input: Handwritten Document Or Handwritten Documents

Output: Binary File

```
Begin
    Read the hand written documents
    doc=0
    While (doc = true)
        binary_file = convertToBinary(handwritten_document)
        binary_file = reverse(binary_file)
```

```
            num_rounds = inputNumRounds()
              for round = 1 to num_rounds do
           // Insert fake value (optional)
                    if sensitive_data_exists then
                        fake_value = inputFakeValue()
                        insertFakeValue(binary_file,
fake_value)
                    endif
                    substitution_chars =
inputSubstitutionChars()
                     substitution_positions =
inputSubstitutionPositions()
                     randomSubstitution(binary_file,
substitution_chars, substitution_positions)
                      binary_file = reverse(binary_file)
                Endfor
            Endwhile
End
```

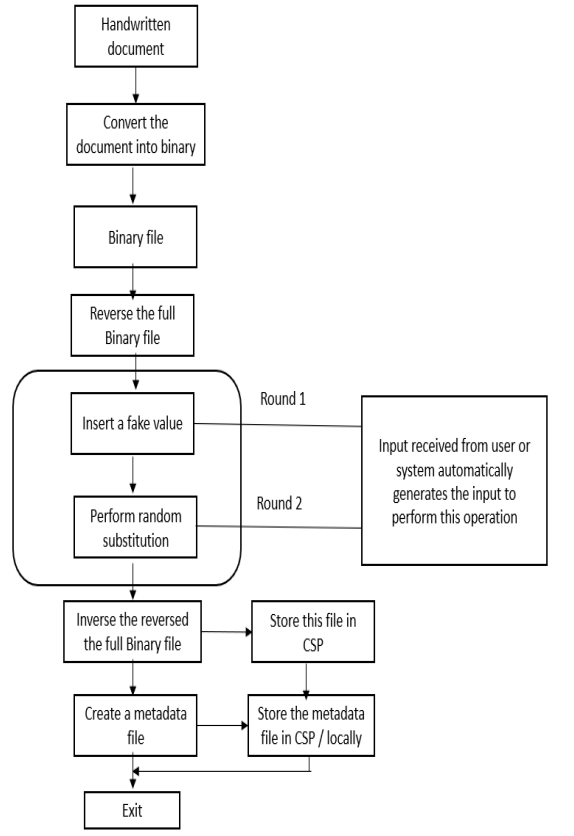

Figure 1: Process flow of the proposed model

The proposed model can be deployed in two ways. Either it can be made customized for a particular user. All the needed inputs like the substitution characters etc. are given by the user. Else these can be calculated by the system using the random number generator method or other appropriate method. The entire details about the substitution etc are stored in a metadata file. This metadata file can be stored in the CSP or the user can store it locally in his own system.

Result Analysis

The proposed method is compared for the speed, security, relabilty and fault tolerance with the existing algorithms. The execution time for encrypting any data using the traditional algorithms is more. Figure 2 gives a graph comparing the execution time taken (in sec or ns???)

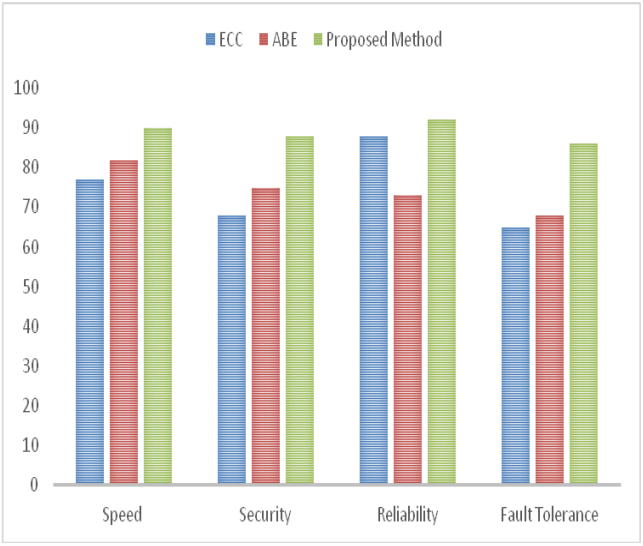

Figure 2 : Comparing the execution time of the proposed algorithm

	ECC	ABE	Multiple Multilevel usercentric Encryption
Speed	77	82	90
Security	68	75	88
Reliability	88	73	92
Fault Tolerance	65	68	86

Table 1 : Comparing the Speed, Security and Reliability

Conclusion

Though cloud computing possesses many benefits, one of the prevalent challenges is the data security issue. The owner of the data losses control over

the data once it leaves his premises. Many models proposed so far uses the traditional encryption method to secure the data. The model proposed in this paper uses a novel encryption model that protects the user's document. The model uses the lightweight approach to safeguard the data. This technique can be used it resource constrained devices. The analysis reveals that the proposed model is found be advantageous when the execution time is considered.

References

[1] I. Gupta and A. K. Singh, ``A confidentiality preserving data leaker detection model for secure sharing of cloud data using integrated techniques,'' in *Proc. 7th Int. Conf. Smart Comput. Commun. (ICSCC)*. Sarawak, Malaysia: Curtin Univ., pp. 1-5,Jun. 2019.

[2] S. Xu, G. Yang, Y. Mu, and R. H. Deng, ``Secure fine-grained access control and data sharing for dynamic groups in the cloud,'' IEEE Trans.Inf. Forensics Security, vol. 13, no. 8, pp. 2101-2113, Aug. 2018.

[3] Z. Zhu and R. Jiang, ``A secure anti-collusion data sharing scheme for dynamic groups in the cloud,'' IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 1, pp. 4050, Jan. 2016.

[4] Cyber Risk Analytics (CRA) and Risk Based Security (RBS). (2021). 2021 Data Breach QuickViewReport.[Online].Available:https://pages.riskbasedsecurity.com/hubfs/Reports/2021/2021%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

[5] A Study Conducted by Ponemon Institute and Sponsored, Analyzed, Reported by IBM Security. (Jul. 2021). 2021 Cost of Data Breach Report. [Online]. Available: https://branden.biz/wpcontent/uploads/2021/08/Cost-of-af-DATA-Breach-Report-2021.pdf

[6] A. Almutairi, M. I. Sarfraz, and A. Ghafoor, ``Risk-aware management of virtual resources in access controlled service-oriented cloud datacenters,'' *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 168-181, Jan. 2018.

[7] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, ``Privacy preserving outsourced classification in cloud computing,'' *Cluster Comput.*, vol. 21, no. 1, pp. 277-286, Mar. 2018.

[8] C.-Z. Gao, Q. Cheng, P. He,W. Susilo, and J. Li, ``Privacy-preserving naïve Bayes classifiers secure against the substitution-then-comparison attack,'' *Inf. Sci.*, vol. 444, pp. 72-88, May 2018.

[9] S. Srisakthi and A. P. Shanthi, "Design of a secure encryption model (SEM) for cloud data storage using Hadamard transforms", *Wireless Pers. Commun.*, vol. 100, no. 4, pp. 1727-1741, Apr. 2018.

[10] A. Al-Haj, G. Abandah, and N. Hussein, ``Crypto-based algorithms for secured medical image transmission,'' *IET Inf. Secur.*, vol. 9, no. 6, pp. 365-373, Nov. 2015.