Multiple Levels of Security for ensuring secure storage of handwritten Documents (MLSD)

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

[1] Assistant Professor, Department of Computer Science, JBAS College for Women (Autonomous), Chennai, India,
Email id: umashiva06@gmail.com
[2]Associate Professor & Head, PG & Research, Department of Computer Science, Dr. Ambedkar Government Arts College (Autonomous) Affiliated to University of Madras, Chennai, India
Email id: amurugan1972@gmail.com

Abstract

In the recent times, there has been an enormous amount of increase in the content that is stored digitally. This storage of information possesses many advantages like reduced manual work, reduction in wastage etc. Though there are enormous benefits, there are some limitations like the security issue. The digitally stored data are vulnerable to a number of attacks. The integrity of the stored information cannot be guaranteed. Many of the handwritten documents are stored in the cloud and these documents often possess confidential or sensitive information. Researchers have worked and developed models that try to protect the digital information. The handwritten documents are one of the digital information that are stored. This paper proposes a MLSD model to protect the handwritten document by making use of cryptographic algorithms. To ensure the integrity of the document multiple levels of security has been used. The proposed system performs experimental analysis of 700 samples of students, which achieves 88%

Introduction

The handwritten document or any digital document's security refers to the measures that are adopted to safeguard the documents. These measures include deploying different tools like using passwords, checking the authentication, providing secured access, etc. All these measures try to restrict the access to such documents. These measures also prevent the document's content from being copied or misappropriately used. It is also possible to protect the document for a particular period of time. This indicates that the document will be available or accessible for a specific duration of time. In addition to these secure parameters, there are measures that can restrict the printing and sharing the content present in the document.

The recent times has seen an increasingly digital world. Hence, it becomes important to ensure the documents are safeguarded. In the case of a security breaches, there is a possibility of sensitive information getting leaked. It may also lead to the situation where the documents get accessed by an unauthorized person. This breach can lead to a loss of the reputation and credibility of an organization There can arise a possibility for a serious legal implication. To secure the virtual or a handwritten document is an important way for a business to secure the confidential data. In the scenario, where a content is published online and the content is distributed digitally, it again becomes more important to ensure that the virtual document is safeguarded.

There is a need to prevent a falsification of the handwriting document images. As this might contain some essential data, the documents need to be protected. Many methods have been developed so as to maintain the origin and authenticity of a given document. This paper proposes a model that can protect the integrity of a handwritten document that is being stored in cloud. The main contributions are as follows:

- The handwritten document is taken as an image file

- The concept of fragmentation is done on the file
- The whole process of encryption is customized as per the user wish
- Added to the encryption, the process of hashing is also included so as to enhance the security measure
- An added security parameter of authenticating the user is added by generating an OTP
- A metadata file is created for all the fragmented file and it is stored using the block chain approach.

Related Work

The handwritten documents are getting stored in a third-party storage. The cloud server acts as the third party and stores the data or the document given by the user. The Cloud computing has acquired a lot of attention during the recent times. It provides flexibility, scalability, reliability, sustainability, and affordability [1], [2]. The vital concept of the cloud is the pay-per-use methodology. It has attracted individuals, organizations and businesses. The organizations and businesses try to benefit from the new approach to make profits [3] – [5].

The security issues faced by the customers of cloud computing are enormous. Researchers have worked together to provide a secure cloud storage. Zhang et al. [6] have analysed the vulnerabilities present in Amazon Machine Images (AMIs). Huang et al. [7] stated in their paper an elaborated study on the IaaS security analysis from the perspective of a stakeholder. Malicious activity can be triggered by the CSP (Cloud Service Provider) or by an attacker.

A number of models have been developed to secure the data and most of these models made use of various cryptographic algorithms [8] The ECC algorithm has been widely used to maintain the integrity of the data [9, 10]. A technique termed as Attribute Based Encryption (ABE) was put forth by Shamir [11]. A mobile application that facilitates the contactless submission of paper-based exams was proposed [12].

Though many models were developed, the user had a very less control over the document. The cryptographic method being used is common for all the users. Hence the chances of getting the stored data through hacking is more. There are also chances of the CSP to turn into a malicious one and attack the data. To overcome this problem, the proposed MLSD method secures the document in such a manner that it is customized for every user.

Proposed MLSD Method

The proposed MLSD method provides multiple levels of security during the storage of a handwritten document.

Multiple Levels Of Security For Ensuring A Secure Storage Of Handwritten Documents (MLSD)

Algorithm: MLSD Algorithm

Input: Handwritten Document Or Handwritten Documents

Output: Encrypted File

Begin
Read the hand written documents
doc=0
While (doc = true)

Virtual_documentConvertToVirtualDocument(Physical_handwritten_document)
Image_document_file ← TakeImageDocumentFile(Virtual_document)

```
                Part1, Part2, Part3, Part4 ← SplitDocumentIntoParts(Image_document_file)
                Hash_value ← GenerateHash(Image_document_file)
               Encryption_algorithm ← GetUserEncryptionAlgorithmChoice()
               Encrypted_part1 ← Encrypt(Part1, Encryption_algorithm)
               Encrypted_part2 ← Encrypt(Part2, Encryption_algorithm)
               Encrypted_part3 ← Encrypt(Part3, Encryption_algorithm)
               Encrypted_part4 ← Encrypt(Part4, Encryption_algorithm)
               Metadata_file1 ← GenerateMetadata(Encrypted_part1, Hash_value)
               Metadata_file2 ← GenerateMetadata(Encrypted_part2, Hash_value)
               Metadata_file3 ← GenerateMetadata(Encrypted_part3, Hash_value)
               Metadata_file4 ← GenerateMetadata(Encrypted_part4, Hash_value)
               Stored_metadata_files_using_blockchain ←
               StoreMetadataUsingBlockchain(Metadata_file1, Metadata_file2, Metadata_file3,
               Metadata_file4)
               User_authenticated ← AuthenticateUserUsingOTP()
      if (User_authenticated):
        Files_uploaded_to_cloud ← UploadFilesToCloud(Encrypted_part1, Encrypted_part2,
Encrypted_part, Encrypted_part4,Stored_metadata_files_using_blockchain)
       Endif
      Endwhile
    End
```

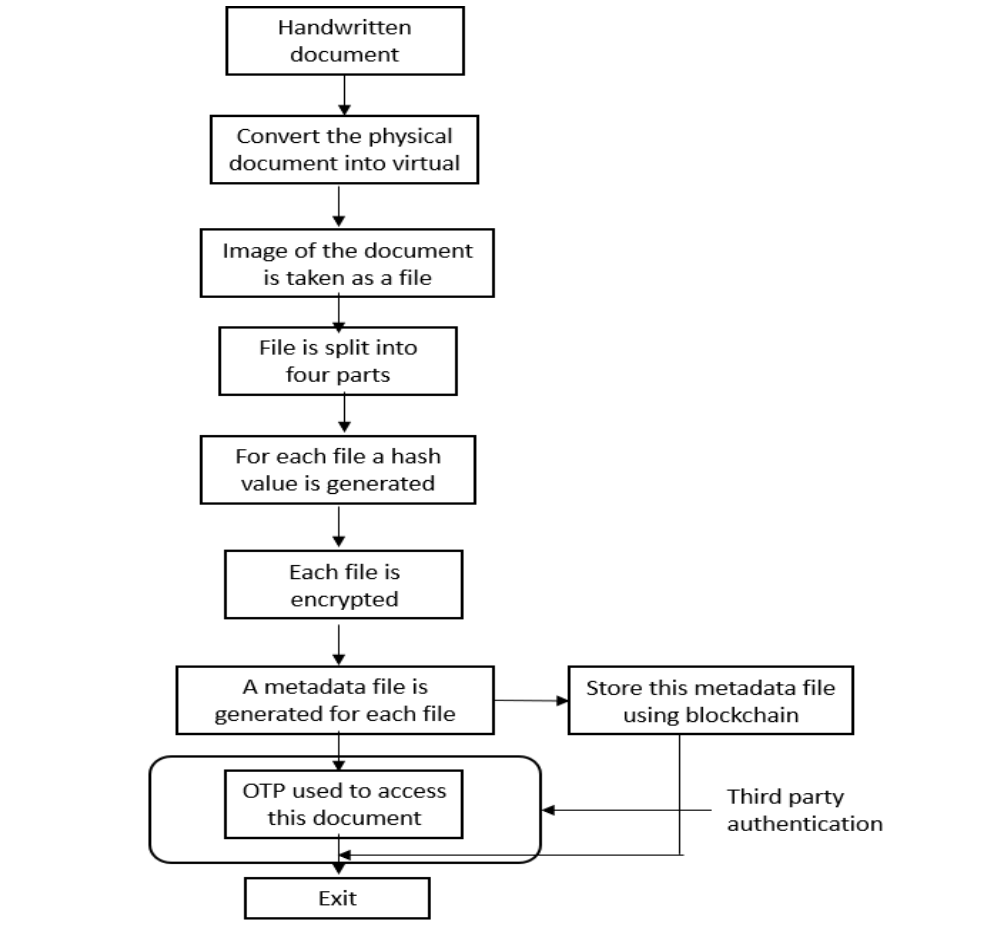

Figure 1. Process flow during uploading of the document

The process flow during the uploading of the document is depicted in figure 1. As depicted in the process flow, multiple levels of security are provided. The multiple levels of security that are provided and their benefits are summarized below

(i) Fragmenting file into four parts – This protects the document as the fragmentation defends against single point vulnerability attack.
(ii) Generating hash value – This value is used to maintain and check the integrity of each part of the file.
(iii) Storing metadata file using blockchain – The metadata file is stored using the blockchain and hence the files are protected.
(iv) Accessing the document – During uploading or downloading the document, the user is authenticated using an OTP.

When the user needs the document, it is possible for the user to download them. The user is first authenticated using the OTP. Next the hash value for each of the file is generated to check the integrity of the file. The user can download all the parts of the file, assemble them in the correct order and decrypt them based on the details stored in the metadata file. Thus, the documents are stored and retrieved in a secure manner.

Result Analysis

The proposed MLSD method ensures security parameter at multiple levels. As multiple levels of security are used, the performance of the system is enhanced. The figure 2 gives a comparison graph depicting the increase in performance when compared to the ECC algorithm.

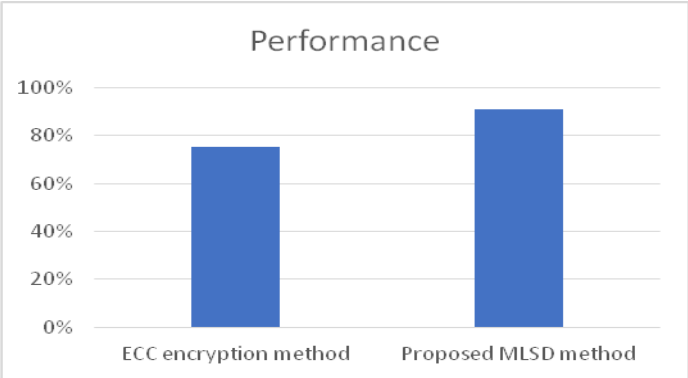

Figure 2. Comparison graph depicting the increase in performance

Conclusion

Thus, this paper proposes a MLSD model that secures the handwritten document. The model uses multiple levels of security during both the uploading and downloading of the documents. The security parameter is customized as per the user's input. This serves as one of the main benefits. When the same security or encryption algorithm is used, it is possible for the hacker to deduce the algorithm. But in the proposed method, the security measures are deployed in a different way for each and every user. This protects the document during its storage and transmission process.

References

[1] T. Vasiljeva, S. Shaikhulina, and K. Kreslins, "Cloud computing: business perspectives, benefits and challenges for small and medium enterprises (case of latvia)," Procedia Engineering, vol. 178, pp. 443–451, 2017.

[2] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, "NIST cloud computing reference architecture," in World Congress on Services, SERVICES, Washington, DC, USA, July 4-9, 2011. IEEE Computer Society, 2011, pp. 594–596, 2011.

[3] S. Becker, G. Brataas, M. Cecowski, D. Huljenic, S. Lehrig, and I. Stupar, “Introduction,” in Engineering Scalable, Elastic, and Cost-Efficient Cloud Computing Applications - The CloudScale Method, S. Becker, G. Brataas, and S. Lehrig, Eds. Springer, pp. 3–21, 2017.

[4] J. Weinman, “The economics of pay-per-use pricing,” IEEE Cloud Comput,vol. 5, no. 5, p. 101,2018.

[5] S. Zhang, X. Zhang, and X. Ou, “After we knew it: empirical study and modeling of cost-effectiveness of exploiting prevalent known vulnerabilities across iaas cloud,” in 9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS ’14, Kyoto, Japan - June 03 - 06, 2014, S. Moriai, T. Jaeger, and K. Sakurai, Eds. ACM, x pp. 317–328, 2015,

[6] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, “The state of public infrastructure-as-a-service cloud security,” ACM Comput. Surv. vol. 47, no. 4, pp. 68:1–68:31, 2015.

[7] Srisakthi, S., & Shanthi, A. P. (Towards the Design of a Secure and Fault Tolerant Cloud Storage in a Multi-Cloud Environment. Information Security Journal, A Global Perspective, Taylor and Francis 24(4-6), 109-117, 2015.

[8] M. Yaghi et al., "Secure Proctoring of Contactless Handwritten-Assessments with Insufficient Computing Resources using Smartphones," 9th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, pp. 302-306, 2022.

[9] S. K. Jemni, Y. Kessentini, S. Kanoun, and J.-M. Ogier, “Offline Arabic handwriting recognition using BLSTMs combination," in *Proc. 13th IAPR Int. Workshop Document Anal. Syst. (DAS)*, pp. 31_36, Apr. 2018.

[10] X. Liu, G. Meng, and C. Pan, “Scene text detection and recognition with advances in deep learning: A survey," *Int. J. Document Anal. Recognit., vol. 22, no. 2*, pp. 143_162, Jun. 2019.

[11] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, “A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11_26, Apr. 2017.