Implementation of Online Document Repository System

[1]G Manoj, [1]Ishan Deep, [1]Kalyani V, [1]Sahana K C, [2]Madhavi R P
[1]UG Student, Department of Computer Science and Engineering, BMSCE, Bengaluru
[2]Associate Professor, Department of Computer Science and Engineering, BMSCE, Bengaluru

Abstract*: The purpose of this document is to present a detailed description of the Online Document Repository System. It will explain the purpose and features of the system, what the system will do, its building blocks, Repository, Advanced Standard Encryption (AES), Digital Signature Algorithm (DSA). This as well explains the technology used for implementation and how the system will react to external stimuli.*

Keywords: ODRS, Repository, AES, RSA, SSL, RDBMS, Signatures.

I. INTRODUCTION

The software system is an online repository system which can record and store the documents which the user owns into its database after being digitally signed by the user or with the help of an agent to achieve non-repudiation. The documents could be electronic records or physical records issued by the government or any affiliated institutions. More specifically, this system is designed to allow a user to manage and communicate with a group of organizations which may need to utilize his documents for a purpose related. A dedicated web portal with a user friendly interface is maintained so as to ease the process of managing the documents. The documents are maintained on a database in a valid format for later access.

II. RELATED WORK

Repository

The system mainly stands on the repository, where the documents are stored. Since we are implementing it on the local host, the repository here would be the file folder on our machine. This would have all the documents that are encrypted and digitally signed. The documents are given a unique ID, corresponding name and its level of visibility (public/private).

Advanced Encryption Standard

This would be our second building block and this forms a part of security, Encryption. The standard that we are using is 256 bit key which takes 10 cycles of repetitions for transformation round. This works on design principle known as substitution-permutation network, fast in both software and hardware. AES is a symmetric key algorithm, wherein the same key is used for both encrypting and decrypting the data.

Signature Algorithm

Once the document is encrypted, it is digitally signed using RSA. This forms the second layer of security. The key generation phase has two parts, one is selecting the algorithm parameters for generation of key that is shared among users and the second one is generating the key pair for single user. The hashing algorithm used is SHA-1.

Secure Socket Layer

The layer comes into picture while the web browser is on the way connecting to the website. A SSL certificate is sent by the server to website on demand, once tis is termed as trusted, an encrypted session is begun. This will allow the encrypted data to be shared between web browser and the server.

III. DESIGN

The Architecture:

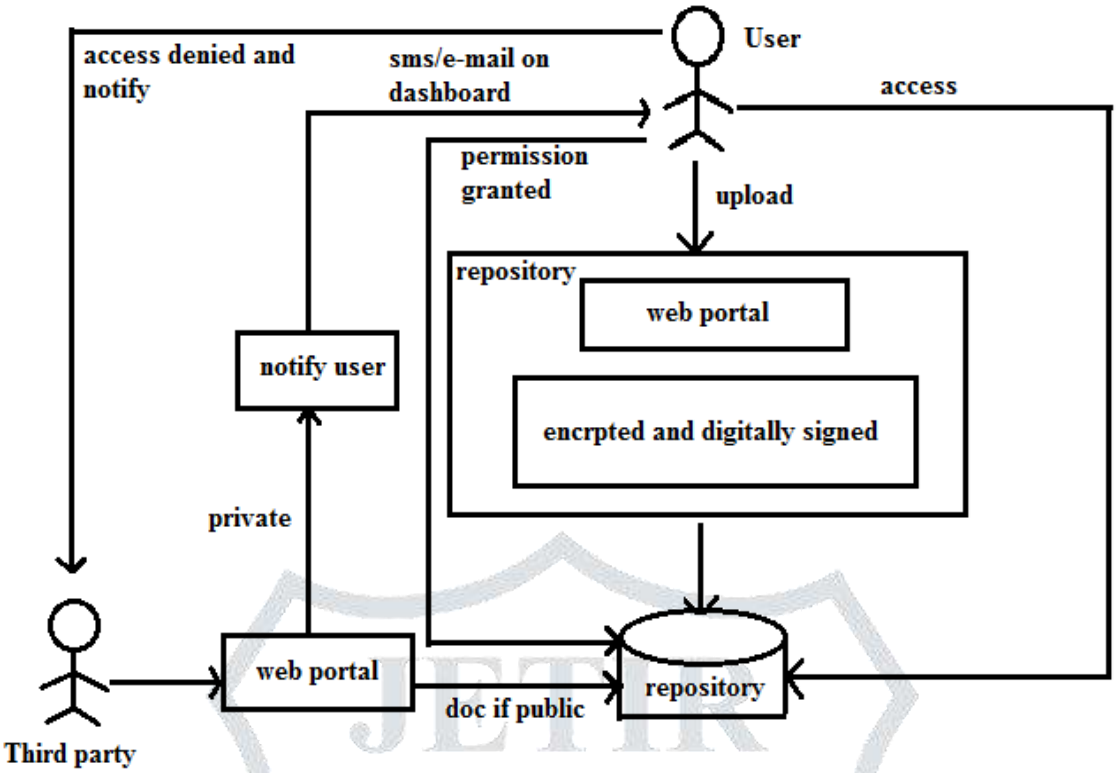

Figure 1. Architecture

Online document repository system [1] basically replaces the conventional method of storing the documents in file systems and a few other already existing Document Management Systems (DMS), where documents are not digitally signed. The repository presented here provides digital signatures as an additional feature. The architecture consists of two actors, the user and the third party organization. On client-side, the registered user, with his login id and password uploads the digitally signed documents to the repository. The three layers of security are implemented on the server-side. The documents are encrypted using AES and then digitally signed using RSA algorithm. Once the documents are signed accordingly, they are stored into the database with a status carrying "SIGNED". On the contrary if the user wishes to upload the documents without signing they carry the status "NOT SIGNED". The documents we are referring here can be of any standard formats such as *.pdf, *.doc, *.docx or plain text (*.txt) files. Also, a number of pictures formats such as JPEG/JPG, PNG, BMP are supported by the system. Upon uploading the documents on the repository are accessible by the user. Similarly, the third party who wishes to view or access the documents can do so if registered with the website. The documents are accessible only if necessary permissions are granted by the owner of the document i.e. if they are made public. If they are private, the organization needs to send a request to the user seeking for the permission to access the data which would notify the user in turn and accordingly, permission is granted.

The certificate creation process:

As shown in the Fig. 2 below, the certification creation process involves the admin who has the authority to verify the details provided by the user like name, address and phone number upon which he creates a certificate for signing for that particular user. When the user wishes to sign his document, he signs the document using this certificate carrying his details. Upon signing this document is uploaded onto the repository carrying the status "SIGNED".

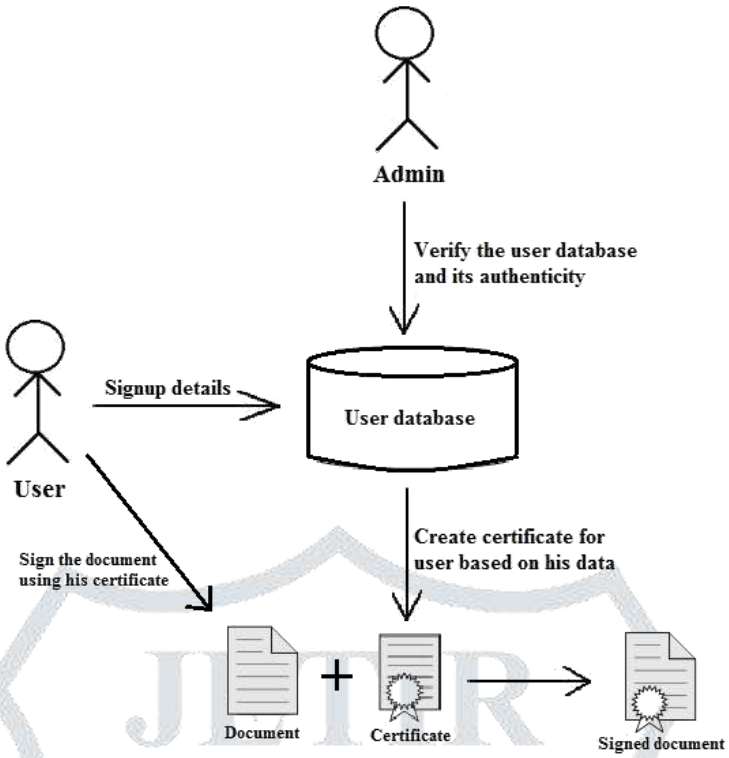

Figure 2. Certificate creation process

IV. IMPLEMENTATION DETAILS

Since this being an online system, all the standard technologies for developing a website were used. Bootstrap framework has been used for designing and appearance purposes. Any available open source IDE such as Eclipse which supports HTML, JSP and java development simultaneously would be ideal for development. Further, since this system handles some confidential documents associated with the user, making this system secure is of the utmost importance and we have taken numerous steps in this regard.

Some of the technical security features we have built in the system are

- Use of Java Server Pages (JSP) instead of plain HTML for security purposes.
- Use of Digital Signature for documents hence avoiding non-repudiation and providing authenticity [2].
- Use of RSA algorithm with a key size of 2048 bits for singing process which is a lot safer and faster as compared to traditional DSA[3].
- Use of AES encryption with a key size of 256 bits for encryption for data on the repository for safety [4].
- Use of Relational DBMS and files as BLOBS (binary large object files) instead of traditional file system [5].
- Use of SSL certificates for the site to prevent man in the middle attack [6].
- Use of OTP based signup for the user to verify the mobile number.

V. CONCLUSION

In this rapid digitizing world, paper-work seems a burden and is also a waste of time and energy. The need for carrying our credentials, wherever necessary, usually hassles the smooth functioning of the process. Our system aims at eliminate the same, with added benefits of backup, non-repudiation and data integrity. The possibilities if implemented on a larger scale are limitless and can ease down the hectic manual work.

VI. FUTURE PROSPECTS

- ***Mobile app development:*** The system explained above would be developed as a cross platform application so that every feature given above can be used from a smart phone running any operating system. The same security features shall be applied when used through a smart phone.

- ***Making the System completely autonomous****:* Currently the system needs a mediator in the form of an admin (or say an authority) which has the resources to verify the user details such as name, address and phone number. Though this acts as a security layer in verifying the authenticity of the user, it is still a burden on the system itself and can be a bottleneck in case the number of users goes high. To prevent such scenarios, it would be appropriate if the background check process happens autonomously by some mechanism and hence would be a good future prospect of this system.

VII. ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1] G. Manoj, I. Deep, V. Kalyani, K.C. Sahana and R.P. Madhavi, "Online Document Repository System", Vol. 3, Issue 3, IJARCSMS, March 2015.

[2] Islam, Rahman, Khan, Hossain, Karim, "Digital signature: does it really work for electronic documents?", Multitopic Conference, Proceedings of INMIC. 8th International, IEEE , 2004

[3] N. Saxena, and N.S Chaudhari, "Secure Encryption with Digital Signature Approach for Short Message Service", World Congress on Information and Communication Technologies, 2012

[4] S. Soni, H. Agrawal, Dr. (Mrs.) M. Sharma, "Analysis and Comparison between AES and DES Cryptographic Algorithm", Volume 2, Issue 6, International Journal of Engineering and Innovative Technology (IJEIT), December 2012

[5] M. Shapiro, E. Miller, "Managing Databases with Binary Large Objects", presented at Mid-Atlantic Association of Oracle Professionals Special Interest Group Conference, unpublished.

[6] N. Liu, G. Yang, Y. Wang, D. Guo, "Security analysis and configuration of SSL protocol", Anti-counterfeiting, Security and Identification, 2nd International Conference, IEEE , August 2008.