International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Design and Implementation of a Digital Signature Solution for Educational Organization

Abinash S [a],GuhanPrasath B[a], Madeshwaran R [a], SaravanaKumar S [a],Nagarasan M[b], Nandhini A[c]

[a]UG Student, Department of ComputerScience and Engineering, Info Institute of Engineering,Kovilpalayam,Coimbatore641107, India.
[b] Assistant Professor, Department of ComputerScience and Engineering, Info Institute of Engineering,Kovilpalayam,Coimbatore641107, India.
[c]Assistant Professor, Department of ComputerScience and Engineering, Sri Ramakrishna Institute of Technology,Coimbatore 641010, India.

A B S T R A C T

In the project titled "Design and Implementation of Digital Signature For Educational Organization".The main objective of the project is to create a secured electronic signature platform.This platform enables the user to sign documents digitally.Earlier credential documents were allowed to sign only in person face to face meetings.But this digital signature platform allows you to sign documents from your place.This digital signature will enable the user easily to sign specific documents digitally in their required areas.

Keywords: Digital Signature,Security,Digital Screens,Two way Authentication.

1. Introduction

This project has been developed keeping in view the security features that need to be implemented in the networks fulfillment of these objectives.To develop an application that deals with the security threats that arise in the network. To deal with the inter-related areas of network security namly Secrecy,Authentication,Non-repudiation and Integrity.

We all have been through a hard pandemic period ,during this period people are not allowed to gather in a place.To overcome the crowd in the colleges,schools and other educational organization etc.. .This digital signature will enable the user easily to sign specific documents digitally in their required areas.

1.1 Project Outcome

The Digital Signature verifies and ensures the document is authentic and comes from a verified source.The document has not been manipulated since it was digitally signed.When a signer electronically signs a document ,the signature is created using the signer's private key.

1.2 Project Impact

The protection of transmitted data from passive attacks.With respect to the release of message contents,several levels of protection can be identified.The broadest service protects all user data transmitted between two users over a period of time.

* *Corresponding author.*
E-mail address: seetharmcon@gmail.com

2. System Analysis

2.1 Proposed System

The project is confirmed to the intranet in an organization. This project has been developed keeping in view the security features that need to be implemented in the networks fulfillment of these objectives.It's cost price is low.Secured approval and completion.We provide to use in many organizations.

3. System Specification

3.1 Hardware Requirements

- DESKTOP OR PC WITH MODERATE PROCESSOR AND OS
- DIGITAL TOUCH SCREENS
- TOUCH PADS
- MOUSE
- DIGITAL PENS

3.2 Software Requirements

- FRONT END SOFTWARES TO CREATE HTML CODE
- CLOUD

3.1.1 Digital Touch Pads

A **signature capture pad** is a device that electronically captures a person's handwritten **signature** on an LCD touchpad using a pen-type stylus. ... Once captured, **digital signatures** can be imported into and used with most ID software and security programs.

Fig .3.1.1. Touch Pad

3.1.2 Digital Pens

A **digital pen** is an input device which captures the handwriting or brush strokes of a user and converts handwritten analog information created using "pen and paper" into digital data, enabling the data to be utilized in various applications.

Fig.3.1.2. Digital Pens

3.2.1 CLOUD

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure. This gives you agility, global scale and durability, with "anytime, anywhere" data access.

4. System Design

4.1 SYSTEM ARCHITECTURE

The signature architecture is based on two ideas.The signature system must read the private keys of users from key stores, and read and update signature logs. Hence, the system's security relies on the confidentiality and integrity of this data. The second idea is to protect these using a secure operating platform.

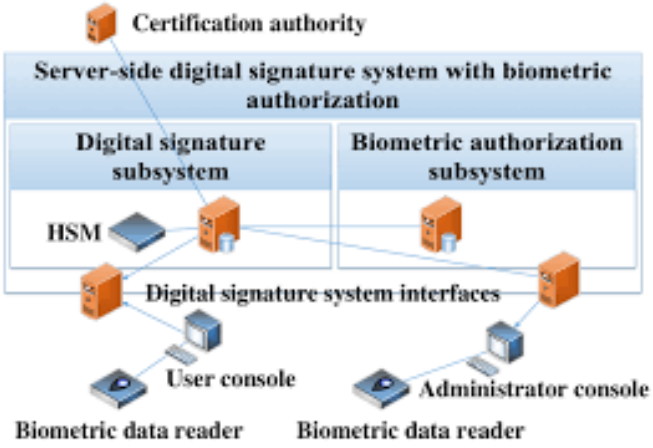

Fig.4.1. System Architecture

4.2 Database Design

The data collected from the Users are stored in the cloud in the following database format.

FIELD NAME	DATA TYPE
Time Stamp	Date and Time
Device Name	Varchar
Channel	Varchar
Document Name	Varchar
User ID	Varchar
Values	Integer

5. Research Design and Method

The study was conducted to evaluate the effectiveness of structured teaching programme and to assess the knowledge and attitude on epilepsy among people living in Kanakarapattu village, Chidambaram Taluk at Cuddalore District in Tamilnadu. Both male and female who are in the age 20-60 years were included in the study. A Total of 30 samples were selected by using convenient sampling technique. The pre test was conducted by using structure interview questionnaire for assessing level of knowledge and 5 point likert scale used for attitude. Then structured teaching programme on epilepsy was given. one week later post test was conducted by using a same structure interview questionnaire and 5 point likert scale.

6. System Implementation

The purpose of System Implementation can be summarized as follows: It making the new system available to a prepared set of users (the deployment), and positioning on-going support and maintenance of the system within the Performing Organization (the transition). At a finer level of detail, deploying the system consists of executing all steps necessary to educate the Consumers on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate, and validating that business functions that interact with the system are functioning properly.

- Planning
- Training
- System testing and

- Changeover Planning

Planning is the first task in the system implementation. Planning means deciding on the method and the time scale to be adopted. At the time of implementation of any system people from different departments and system analysis involve. They are confirmed to practical problem of controlling various activities of people outside their own data processing departments. The line managers controlled through an implementation coordinating committee.

The committee considers ideas, problems and complaints of user department, it must also consider.

- The implication of system environment
- Self selection and allocation form implementation tasks
- Consultation with unions and resources available
- Standby facilities and channels of communication

7. System Testing

Testing is the process of running a system to verify that it meets specified requirements and to find the errors. In this site, testing enhances the integrity of a site by detecting deviations in design and errors in the site. It verify through testing of every input in the application to check for desired outputs. The implementation is the final and important phase. It involves system testing in order to ensure successful running of proposed system.

8. Output and Processing

The Users Will Login Using His Specific User Id And Password.

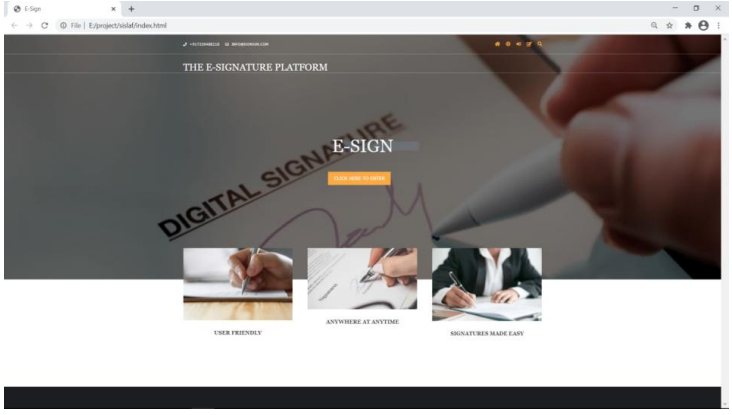

Fig 7.1 The Signature Platform

Users Will Be Allowed To Fill and Sign The Form Further

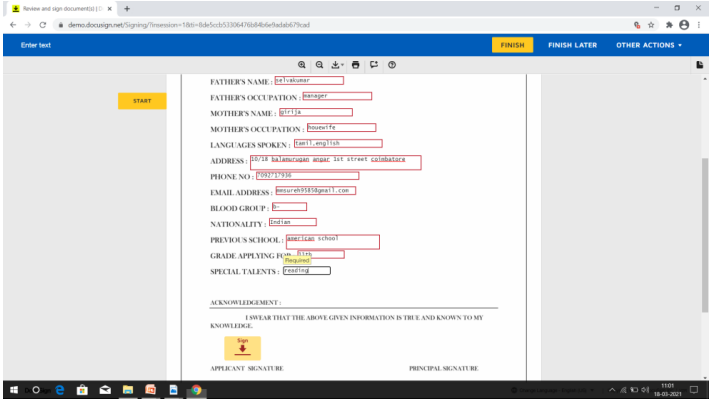

Fig 7.2.Form Filling Page

User Will Have Styles And Procedures To Adopt Their Signatures

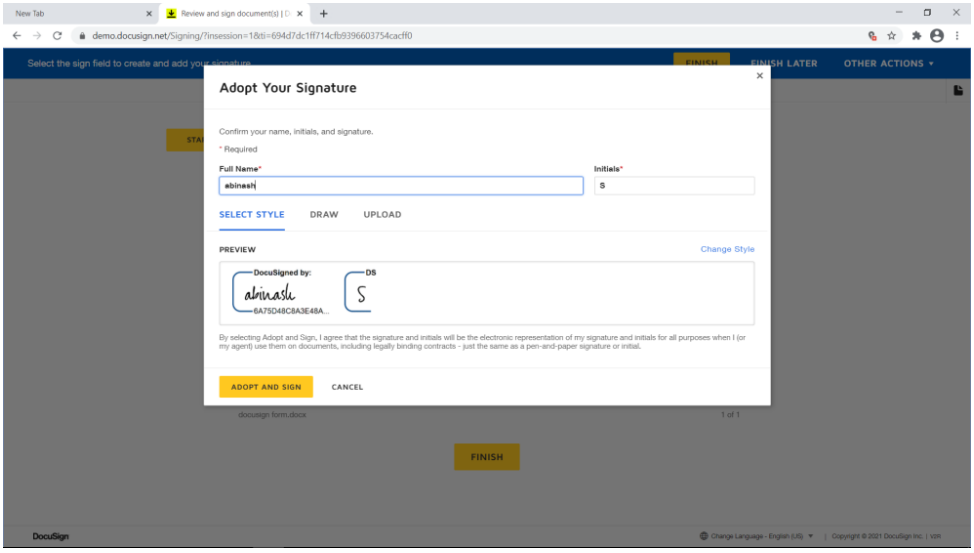

Fig 7.3.Signed Document And Styles

A Document Will Be Sent To Both User And Admin For Further Verification

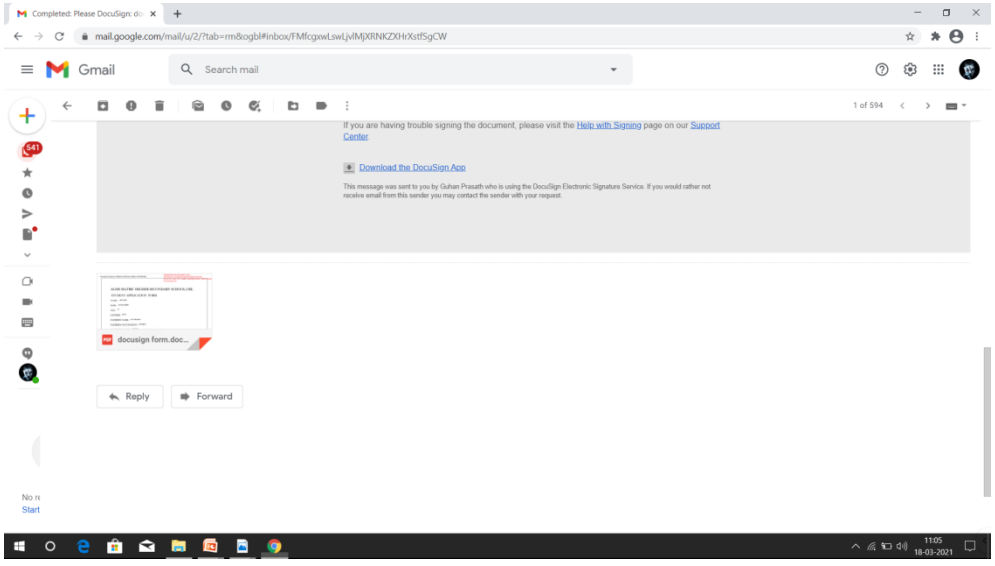

Fig.7.4 Verification and Sending Documents to User

9. Conclusion and Future Enhancement

8.1 Conclusion

Digital Signatures are difficult to understand.Digital Signatures will be championed by many players that the public distruts,including national security agencies,law enforcement agencies,and consumer marketing companies.We conclude that this will create new era of signatures.

8.2 Future Enhancements

This Signature platform will enable users around Globe to sign documents from DoorStep in Future days.This will create immense growth among e-sign procedures. This can also be modified according to all needs and required areas. This design can serve a great social cause.

REFERENCES

[1] Carlisle Adams and Guy-Vincent Jourdan, "Digital Signatures for Mobile Users", 2014 IEEE Conference, Toronto, Canada.

[2] Shahzad Alam, Amir Jamil, Ankur Saldhi, Musheer Ahmad , "Digital Image Authentication and Encryption using Digital Signature", 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India

[3] Emir Husni, Bramanto Leksono , Muhammad Ridho Rosa , "Digital Signature for Contract signing in Service Commerce",2015 International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E) Samosir Island, North Sumatra, Indonesia, September 7-9, 2015 .

[4] Shivendra singh, Md. Sarfaraz iqbal, Arunima Jaiswal,

[5] "Survey on Techniques Developed using Digital Signature: Public key Cryptography," International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 16, May 2015.

[6] Alpizar-Chacon, Mario Chacon-Rivas, "Authenticity and versioning of learning objects using the digital signature infrastructure of Costa Rica", 2014.

[7] Mauro Conti, Nicola Dragoni, and Viktor Lesyk , "A Survey of MAN-IN-THE-MIDDLE attacks" 2015 IEEE Communication Surveys & Tutorials.

[8] Shaun Stricot-Tarboton, Sivadon Chaisiri, Ryan K L Ko , "Taxonomy of MAN-IN-THE-MIDDLE attacks on HTTPS", 2016 IEEE TrustCom-BigDataSE-ISPA .

[9] Niraj Kumar, Pankaj Gupta, Monika Sahu, Dr. M A Rizvi, "Boolean Algebra based Effective and Efficient Asymmetric Key Cryptography Algorithm: BAC Algorithm", 2013 IEEE.

[10] Richard Bassous, Huirong Fu and Ye Zhu, "Ambiguous Asymmetric Schemes", 2016 International Conference on Computational Science and Computational Intelligence.