Document Validation and Verification System

Samit Shivadekar (IT, SIES GST, Navi Mumbai, India,)
Stephen Raj Abraham (IT, SIES GST, Navi Mumbai, India,)
Sheikh Khalid (IT, SIES GST, Navi Mumbai, India)

***Abstract*— 'E-Governance system' will be an online platform for deliverance of Government to Citizen Services and storage of digital certificates, documents etc. The system consists of a DigiVault [Digital Storage] website which can be linked with different websites of various government departments. In this Project the Documents generated by the government will be digitally signed and verified by government authority entitled for the same. Digital Signature of documents will be implemented through Public Key Infrastructure. Certificates serve as identity of an individual for a certain purpose, e.g. a driver's license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet. Document Validation will be provided at the user end where he wants to apply for certain governments documents like Pan Card and Licenses.**

***Index Terms*—Digital Signature, Validation and Verification.**

I. Introduction

1.1 Document Validation And Verification

Imagine yourself as a person who urgently wants a particular certificate from some government authority. You have never visited a government office before. You visit that government office and see a huge rush and lengthy queues. You move from counter to counter enquiring how you can acquire that certificate. Visiting a government office to seek service is cumbersome. Thus arise a need of E-Governance system where Government to Citizen Services will be provided over electronic system and Internet which is convenient to citizens as well as government officers'-Governance system will consist of a website having a Digital Vault facility for every user. Digital Vault will be a cloud repository from where memory will be allocated to every user. A user will have to Register on this website and use this login credentials to apply for a certificate on other website. The certificate authority will then process the application and will then upload the E-Certificate to the user account which can be accessed from Digital Vault directly. The concept in short is "Apply for Service on different locations and access the Service from single location". Thus the process is no more time consuming like the traditional way to acquire certificates from government offices. Moreover, Government authority thus delivers E-Certificate on Digital Vault from where a user can access, download and print this certificates which is digitally signed & verified by the Government agent appointed for the same. These certificates will have a digital signature and will be self-attested.

1.2 Digital Signatures

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, Brazil, Saudi Arabia, the European Union and Switzerland, electronic signatures have legal significance.

Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through a nonsecure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Thus Digital Signatures provide the following three features:-

Authentication- Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.

Integrity - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions.

Non Repudiation – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

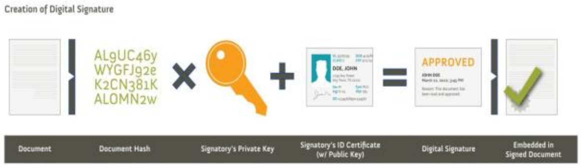

Fig 1.1 Digital Signature in Documents

A digital signature scheme typically consists of three algorithms;

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.

2. Aim of the Project

- Reduce operational complexities and delay among various agencies of the Government.
- Helps cost curtailments from the national as well as the state level budget grants.
- Reduces the corruption rate in the governmental transactions.
- Increases the efficiencies of various departmental activities of the Government. As the chance of human interventions get reduced within the governmental operations, the scope of occurrence of human errors either intentional or unintentional get decreased.
- Tighten the national security from the perspective of infiltrations and cross border terrorism.

3. Document Validation

The users on this website will be both administration team/certificate issuing government authority as well as normal users seeking service. User will upload the documents & the Software at the Server End will validate the documents by processing the documents with the help of Optical Character Recognition (OCR) Software. OCR will convert extract the required details from the uploaded Documents and that extracted text will be compared with the data entered by the User while applying for the Document. For further confirmation if both the data matches then Document Identity Number will be verified from the respective company so as to confirm the user's Documents. If all is Fine then the document can be made for the user and he/she will soon get the requested document.

4. Proposed System:

Document Validation: Our prototype system will consist of two such websites of different government departments. Both the website will have a registration/login component for authentication of users. The users on this website will be both administration team/certificate issuing government authority as well as normal users seeking service. User will upload the documents & the Software at the Server End will validate the documents by processing the documents with the help of Optical Character Recognition (OCR) Software.

Document Verification System by Digital Signature: The Documents generated by the government will be digitally signed and verified by government authority entitled for the same. Digital Signature of documents will be implemented through Public Key Infrastructure. A Digital Signature Certificate is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. Digital certificates are the digital equivalent (i.e. electronic format) of physical or paper certificates.

5. System Objectives

The Primary objective of our project is to simplify the process of accessing government to citizen services and make it hassle free. It will also save efforts of government officers to deliver these services.

• Minimize the use of physical documents.

• Ensure Authenticity of the e-documents and thereby eliminating usage of fake documents.

• Secure access to Govt. issued documents through a web portal.

• Reduce administrative overhead of Govt. departments and agencies and make it easy for the residents to receive services anytime, anywhere access to the documents.

• Enable e-Signing of documents and make them available electronically and online.

6 .Figures

6.1 Flow Diagram:

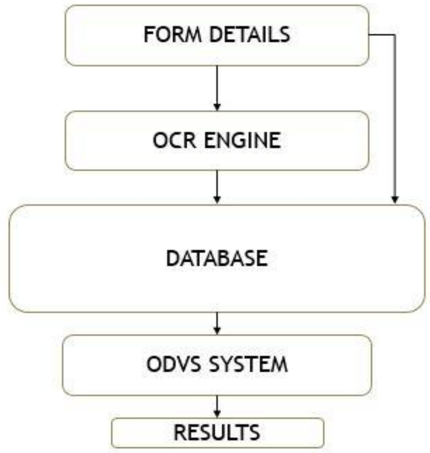

FIG 6.1 FLOW DIAGRAM OF DOCUMENT VALIDATION SYSTEM

6.2 DATAFLOW DIAGRAM

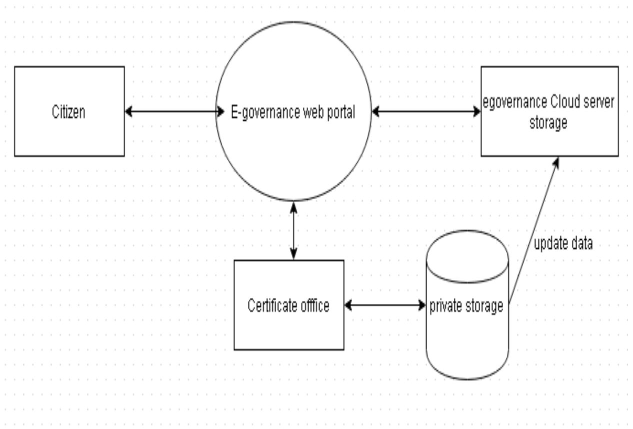

FIG 6.2.1 LEVEL 0 - DATA FLOW DIAGRAM

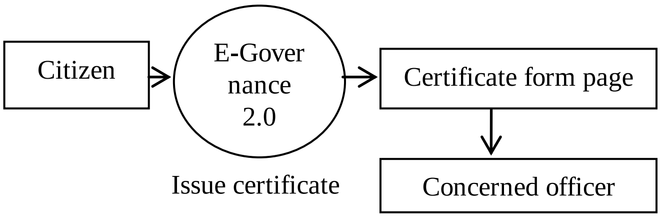

FIG 6.2.2 LEVEL 1 - DATA FLOW DIAGRAM

6.3 CLASS DIAGRAM

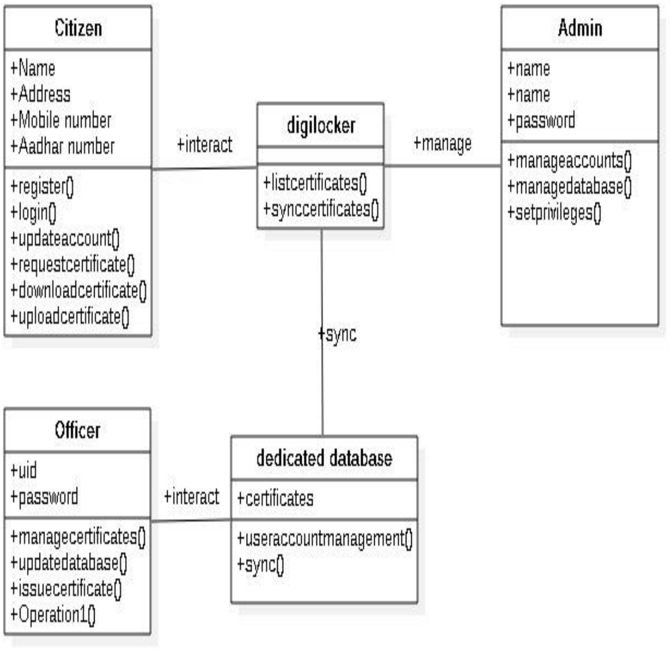

FIG 6.3 CLASS DIAGRAM OF DVVS

5. CONCLUSION

We were able to fully construct an application can Sign the Documents Generated by the Government with the help of Digital Signatures.OCR Application that can be used to find whether the documents given by the user to access the government Documents were valid or not.

ACKNOWLEDGMENT

. We express our deep gratitude to our project guide Mr. Samit Shivadekar for providing timely assistant to our query and guidance that she gave owing to her experience in this field for past many year. She had indeed been a lighthouse for us in this journey. We extend our sincerity appreciation to all our Professor from SIES GST for their valuable inside and tips during the designing of the project..We are also grateful to our HOD Mrs. Leena Ladge for extending her help directly and indirectly through various channels in our project work.

REFERENCES

[1] Prabhu C.S.R. (2004), “e-Governance: Concepts and Case Studies”, Prentice Hall of India Private Limited, New Delhi, India.um

[2] Perri-6 (2004), “e-Governance Styles of Political Judgment in the Information Age”, Palgrave Macmillan, London.

[3]http://www.academia.edu/3742047/IMPLEMENTATION_OF_AUTHENTICATION_IN_E-GOVERNANCE_-_AN_UML_BASED_APPROACH

[4]Proposal-PKI-Digitised-Signature-for-IWDMS_Kar-tikShashtri_31Jan2011
implementing-public-key-infrastructure-pki-microsoft-windows-server-2012-certificate-servic-35427

[5] A Practical Deployment Strategy for Digital Signatures and Seals
http://www.scribd.com/mobile/doc/135811020/Digital-Signature-Project-Report

[6] http://www.e-mudhra.com/e-tender.html

[7] Digital Signature Scheme with Message Recovery Advances in Computer Engineering (ACE), 2010 International Conference

[8] http://www.cca.gov.in/cca/

[9]https://en.wikipedia.org/wiki/Optical_character_recognition

[10] https://en.wikipedia.org/wiki/Tesseract_software

[11] Mori S, Ricoh, Yokohama, Suen,Yamamoto K "Review of OCR research and development" Proceedings of the IEEE Volume 80-7 pp. 1029 – 1058 2002

[12] Shijin Lu, Linlin Li, Tan, C.L. "Document Image Retrieval" Pattern Analysis and Machine Intelligence, IEEE Transactions Volume 30-11 pp. 1913-1918 2008

[13] Zagoris K., Papamarkos N., Chamzas C "Web Document Image Retrieval System"Image Processing IEEE International Conference pp. 477-480 2006.

[14]
http://www.icisa.cag.gov.in/images/Guidelines_for_Usage_of_Digital_Signatures_in_e-Governance_Ver.1.0.pdf

AUTHORS

Prof. Samit Shivadekar
Professor at SIES Graduate School Of Technology.

Mr. Stephen Raj Abraham
B.E, Student at SIES Graduate School Of Technology.

Mr. Sheikh Khalid
B.E, Student at SIES Graduate School Of Technology.