An Approach for Securing Data in e-Governance Projects in Developing Countries

Rakhi V. Pathrikar

National Informatics Centre, Ministry of Communication and Technology, Government of India

Abstract: ***A digital signature is an electronic form of a signature that can be used to authenticate the identity of the signer of the data .It means that the signer cannot easily disclaim it later. It ensure that the original content of the data is not tampered. As a part of e-Governance, many application software implemented for Government of Maharashtra. Huge data is generated through application software and it is stored on the database server in State Data Centre (SDC) , still data security, privacy is the main concern. Data management cannot fully trusted by application software or database administrators. Hence there was immediate need to develop innovative, technological and strategic solution. In this paper I have presented method for data security by using digital signature. User of the application can sign data with his own digital signature on USB token. The next level of user can verify the signed data and certify the changes. This method can be integrate in any work flow based eGovernance application for data security. Data signing and verification is the process which can be used for a single data row or bulk data. Implementation or usage of this component is all depend on the requirement of development team or adaptive. Development team can use it in the application work flow as suitable.***

Keywords: digital signature, data signing , verification, eGovernance, hashing

1. Introduction

This signing and verification of data plays an important role in information systems where maker/checker concept is implemented. The principle of **maker** and **checker** means that for each transaction**,** there must be at least two individuals necessary for its completion. This paper evaluates an approach for data signing and verification in such work flow based application software.

Digital Signature is a process that guarantees that the data have not been altered or tempered in transit.

Mutation entry in 7/12 extract is the best example of such type of systems. Mutationis the recording of a transfer of title of a property from one person to another in the revenue records.In rural areas ownership of a particular land can be established on the basis of 7/12 extract. It is called as Record of Rights(ROR).Mutation entries are generated at Tehsil officeand mutation entry is certified by the Circle officer and ROR is updated

2. Literature Survey

eSign service by CDAC, Pune India[1] The objective of eSign service is to offer on-line service to citizens for instant signing of their documents securely in a legally acceptable form. Two major challenges involved are (a) authentication of the user and (b) Trusted method of signing. Aadhaar based authentication is carried out to address the first challenge and Public Key Infrastructure (PKI) is used to securely sign the user document and establish the trust

Rachana C. R. [2] digital signatures provide the following advantages: 1. No need to print out documents for signing; 2. Reduced storage of paper copies; 3. Improved management and access (anytime/anywhere) of electronic versus paper documents; 4. Elimination of need for faxing or overnight mailing—reduction of cycle time; 5. Improved security of document transmission;.

NeGP [3] With the implementation of the National eGovernance Plan (NeGP), more and more Departments/Line Ministries in India are automating their operations and business processes and making their Service delivery online. As a result, electronic documentation is slowly permeating every aspect of the business workflow in the Government Departments. However when a signature authorization is required on a document, a hard copy is printed to get a physical routing of signatures.

Yuh-Min Tseng a,*, Jinn-Ke Jan b, Hung-Yu Chien b[4]-proposed a digital signature scheme using self-certified public keys in the ISP era. It provides the message recovery property. The authenticated encryption scheme only allows a specified receiver to verify and recover the message. The authenticated encryption scheme with message linkages is suitable for transmission of large message, while providing the linkages among signature blocks.

It is all about securing documents, messages, authentication using digital signature. But there is need to secure data in information systems in eGovernance Projects

This paper presents a fast and flexible method for data security. This method takes hash of transaction data as input, digitally signs it and signed data is stored in the database for further transactions.

3. Proposed Work

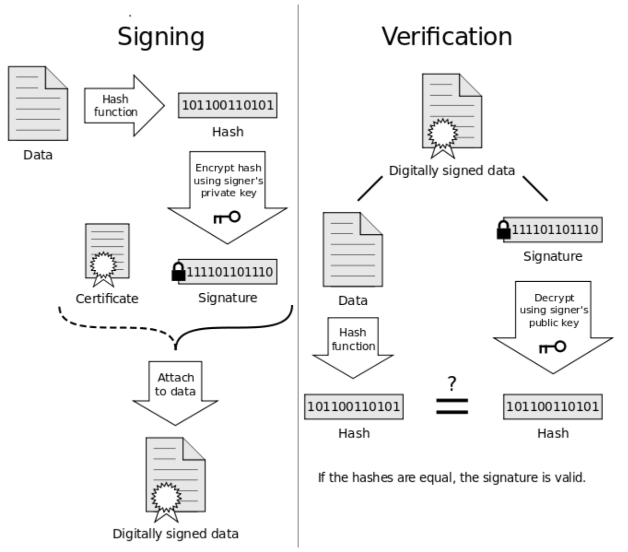
Problem Statement

The problem is that Database servers are there in state data centres .Data stored in any open source database like Postgres should not be tampered by unauthorized access and by unauthorized roles and also outside the boundaries of the application software. To prevent this problem , I have implemented the concept of digitally signed data. Digital signatures enable the authentication and assuring the recipient both the identity of the sender and the integrity of the data. Secondly in many eGovernance projects where it is expected that user should use his own digital signature token. So user should able to sign data or document in a work flow based system.

4. Module Description

Methods / Approach

Data Signing and Verification – Conceptual Diagram



This project is mainly depended on client/server model. The system is divided into three parts:

1) Any web based application running on Server
   The application should be able to generated data which is to be signed and send it to the client application for signing.
2) Data signing Client component
   The web based application requests the client and client component responses by sending data to the servers request.
3) Actual data signing procedure by user with Digital signature Token attached to users desktop/laptop
   RSA DIGITAL SIGNATURE ALGORITHM : The RSA Digital Signature algorithm is a FIPS approved cryptographic algorithm for digital signature generation and verification.

Token Registration
First token registration is done before actual usage of digital signature token , details gets register in the data base which is there in the server. Actual signing and verification process has three components

Data hashing
Most widely used SHA-1 cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST is used for creating hash of the data . SHA-1 produces a 160-bit (20-byte) hash value. This value can be generated in the application or at the database side.

Data Signing
Once Hash value is generated it is send to client component for data signing.
Microsoft's RSA algorithm is used for data signing.
The client component send the signed data to the server.

Data verification
If the signed value and the hash of the data that is to be verified is compared and it matches then true is returned else false is returned

5. Result

Consequently, I found that the component provides a well-defined and efficient result depends on each situation I assumed. The component is made simple to use by the user that does not have background in the digital sign technique. Component is so flexible that it can suit to any eGovernance application. This component is implemented for eMutation project of Department of Land Records, Government of Maharashtra

- There are 44000 villages in Maharashtra with 2.5 crores ROR records Currently 1.5 crores ROR records are signed
- Daily approximately 15000i.e Monthly 4.5 lakhs ROR records get signed

6. Conclusion

In this paper, I proposed a model for the data signing and verification for web based eGovernance application. I used Microsofts alogorithm and digital signature to achieve the concept. As results, I found that the component worked well. Citizens also benefitted since , digital signatures can provide added assurances to identity and tamperproof data.

When it comes to exchange data from application to application or data is to be given to outside agencies like Income Tax department , only secured and non tampered data will be exchanged Component is on Microsoft platform still it can be invoked through any non Microsoft applications like PHP , Java. Only limitation is that , browser should support Activex Component .

7. Future Scope

Implementation of data signing and verification component in all eGovernance information systems. Efforts should be made to secure data in cloud. The main objective was to secure data . The approach used for the encryption in the verification process was the digital signature. In the implementation we used as an example of the data coming from application softwaret, this research is not covering other various kinds of data sources .

References

[1] CDAC esign web site https://esign.cdac.in/
[2] International Monthly Refereed Journal of Research In Management & Technology
[3] ISSN – 2320-0073 Volume II, March'13
[4] Guidelines for Usage of Digital Signatures in e-Governance by Government of India , Department of Information, Technology Ministry of Communications

and Information Technology Government of India

[5] Yuh-Min Tseng a,*, Jinn-Ke Jan b, Hung-Yu Chien b[5]- proposed a digital signature scheme using self-certified public keys in the ISP era. It provides the message recovery property. The authenticated encryption scheme only allows a specified receiver to verify and recover the message. The authenticated encryption scheme with message linkages is suitable for transmission of large message, while providing the linkages among signature blocks.

[6] Articles from Microsoft TechNet