E-ISSN: 2278 – 179X

Journal of Environmental Science, Computer Science and Engineering & Technology

Available online at www.jecet.org

Engineering & Technology

Research Article

Security Framework for National electronic Document Repository (NeDR)

Narendra K Pareek[1], Vikas Agrawal[2] and Prashant Mittal[2]

[1]University Computer Centre, Vigyan Bhawan M L Sukhadia University,

Udaipur (Raj) India.

[2]National Informatics Centre, NW-Block, Secretariat

Rajasthan State Unit, Jaipur (Raj.) India.

Received: 15 March; 2012; Revised: 25 March 2012; Accepted: 30 March 2012

ABSTRACT

In India alone huge vegetation is destroyed every year to manufacture paper which is used as base material for retaining copies of the documents. Other environment hazards associated with the copying industry is large consumption of toner and power. Receivers have to invest a lot in infrastructures to store the documents, that too seldom been retrievable at least in the case of public authorities. The proposed solution not only overcomes these issues but also helps in better service delivery, enhanced security of documents and profitable business opportunities to SMEs particularly in rural areas. Sustainability of CSCs and Rural IT kiosk is of great concern, as long term support by government would not be possible, and these establishments/ entrepreneurs have to be equipped with enhanced service delivery and increased footfalls. Such a solution has to be reliable one and information security has to be dealt on priority.

Keywords: e-Gov, Rural IT, cryptography, Digitized document, Ciphering, Digital signature.

1. INTRODUCTION

Although more and more services are being opened for citizens through ICT based communication channels under the ambit of e-Gov, still large volume of paper based documents are being generated around us every day. Knowingly or unknowingly, one attaches large chunk of photocopies along with his/her application. This not only taxes him/her in the form of photocopying charges and postal charges but also costs environment in the form of loss of green assets resulting in increase in chemical wastages. Over and above this, he/she has to wander around for getting these documents attested every time he/she uses a fresh copy. Security of the these valuable documents in possession is another concern, often loss of

the documents causes lot of difficulties, wastage of money and time in getting duplicate issued from the origin.

Government is investing handsome budget on building ICT based infrastructure in rural area through its flagship programmers', and lot of discussions are going on by practitioners and planners to build a favorable environment for their sustenance through rolling out more and more applications, meaningful contents and doorstep services. Though, these would require process re-engineering, legal acceptance and changes in regulatory practices but once accepted by rural masses it would make the business of setting up rural IT kiosk profitable and sustainable.

2. NATIONAL ELECTRONIC DOCUMENT REGISTRY – FRAMEWORK

National electronic Document Registry (NeDR) is being proposed here as an authenticated, authoritative central repository of the digitized documents. Each document with NeDR would be having Unique Document Identification Number (UDID), and further usage/retrievable of documents would be possible using UDID pertaining to the document. Users of the NeDR services would have to pay a marginal amount for the retrieval of digitized documents. The nodes, here CSCs/ Rural IT kiosk, would be authorized to scan and digitally sign the documents, and they would also be allowed to charge against these services. The document holder would be allowed access by mentioning the UDID and its access code if so attained depending on the limited access allowed. The additional security features as Safe Deposit Vaults (SDV) for Documents may also be built, where encrypted document could be accessed by the private key only. NeDR would also keep track of the users and add up the credentials of the document as more and more of the same is used.

Stakeholders: First and foremost stakeholder would be citizen, who would be getting relieved from the burden of paper based copies of the document on one hand and would make him/her capable to submit the document online, if so facilitated by other party.

Second and crucial stakeholder would be regulatory bodies, who would accept the digitized document and shall govern the processes involved in document encryption, storage, retrieval, authorization of service providers and usage charges. Some sort of formal regulatory body may also be constituted to act as Big Brother. This group of stakeholder would own the responsibility of process of re-engineering.

Third and still important component would be Authorized Service Providers (ASP) who would be having infrastructure at remote locations. Panchayat Raj Institutions are already creating this at block and gram panchayat levels as "Rajiv Gandhi IT Seva Kendra". Each ASP would be using its Digital Signature (DS) for digitally stamping the contents being kept in NeDR.

Fourth one would be the document users, to whom citizens would be submitting the UDIDs along with access rights. This would include government as well as financial institutions and private players. Considerable contributions would be formed as collection of usage charges from these players. Environmental credits may also be associated with user domains to promote reduction in paper usage.

Last but certainly not the least would be the communication channel providers as this would be the backbone of the NeDR framework. BSNL, being the state owned Telecommunication agency is committed to connect the gram panchayats through Broad Band. Certain other alternatives like 3G and WiMax may also be explored for better service delivery to rural entrepreneurs. The telecom regulatory authorities would be requested to promote conducive environment for other players for building high speed infrastructure for digital communication, however present available resource shall first be used up to its optimum capacity.

Technology: The solution has been explored here using less technology yet secures service oriented architecture, which is lighter enough to be deployed as not so resource intensive applications at remote nodes. The central repository would have to be robust one and should be under government control

completely. Necessary and sufficient security and disaster recovery arrangements shall also be associated with it.

The privacy concerns would be taken care of by the system. The documents would be categorized in four or more categories depending on its contents, to start with "Private", "Secured", "Protected" and "Public" [1]. The documents under these categories will be having different methods of authentication, ciphering technologies and access mechanisms.

The one which is under "Private" category would use symmetric method of coding where the user/owner would code/decode his/her document/image using own digital signature. Second one "Secured" would use asymmetric ciphering, where the document could be deciphered using his/her public key which will be accessible to authorized user group. "Protected" document would be simple codified documents by ASP's own digital signature but could be accessed by the authorized users. Last one category of document "Public" would be codified by the ASP's DS and would be accessible to public.

Solution Acceptance: Proposed idea may have numerous obstacles to accomplish for its success. But as more and more awareness is creeping in masses towards ecological and environmental hazards, excess paper and carbon usage being part of it, would be the key points to attract attention. The faith will be built showing the ICT interventions, the subsidiary benefits would be savings towards cost of storage space for document preservation, security, and time savings etc.

To overcome the inertia of the existing notary domain, the government/financial institutions would be prompted to extend soft loans for upgrading their setup and to adapt the new system as it has been done while implementing CNG buses in metros.

3. BUSINESS MODEL

Nothing gets propagated in the market until it seems economically viable; the project has been evaluated by the IT experts and has been short listed as workable ones. However, more rigorous efforts have to be put on before roll out to ensure flaw less implementation. The savings through this project would be enormous if environment protection could be quantized in economical terms, as it would be saving huge vegetative cover on earth. Savings in the form of Carbon Credits, postal and document handling charges would also be considerable and surely attract the users.

NeDR Service Protocols: NEDR has been built on Service Oriented Architecture (SOA). Once accepted, it could also be linked with other e-Gov applications for document handling, thus relieving individual application to take care of the supportive documents. NeDR web services could be easily integrated with any contemporary technical solutions. It uses standard encryption algorithms, which could be vetted through the designated authorities.

Processes Involvement: Realization of NeDR framework requires following basic processes.

(a) Solution building
(b) Core infrastructure setup
(c) Regulatory changes
(d) Creation of ASPs
(e) Public awareness

Suggested prototype solution has already been developed and tested, it would require considerable enhancements. The central infrastructure has to be built capable enough to serve the large chunk of users. Subtle regulatory changes have to be incorporated to accept these digitized documents. ASPs in similar line of Notaries have to be authorised as public interfaces of NeDR. Reaching up to this height, public awareness has to be created through all means of communication to kick start the usage of NeDR services.

4. CRYPTOGRAPHIC ALGORITHMS

Security is an important issue in communication and storage of digital data. To protect digital data from unauthorized eavesdropper, several techniques are available. All these techniques fall into three different categories [1] – watermarking, steganography and cryptography. Among these, cryptography has become one of the major tools to provide high level of security. The actual mathematical function used to encrypt and decrypt messages is called a cryptographic algorithm or cipher. Each type of data has its own features, therefore, different cryptographic techniques should be used to protect data from unauthorized users. In the last few decades, several encryption algorithms based on different principles and techniques like chaos based, number theory, combinatorics etc have been suggested.

Restricted algorithm: If, as most historical ciphers, the security of the message being sent relies on the algorithm itself remaining secret, then that algorithm is known as a restricted algorithm. These algorithms have a number of fundamental drawbacks.

Key-based algorithm: All modern cryptographic systems make use of a key. Algorithms that use a key system allow all details of the algorithm to be widely available. This is because all of the security lies in the key itself only. With the key based algorithm, the message is encrypted and decrypted by the algorithm which uses a certain key, and the resulting encrypted message is dependent on the key and not on the algorithm. This means that eavesdropper can have a complete copy of the algorithm in use but without the specific key used to encrypt that message it is useless. All key-based algorithms fall in two categories:

Symmetric algorithm: Symmetric algorithms have one key that is used both to encrypt and decrypt the message. In order for the recipient to decrypt the message they need to have an identical copy of the key. This presents one major problem- either the recipient can meet the sender in person and obtain a key that way or the key itself must be transmitted to the recipient and is thus susceptible to eavesdropping. Based on the structure of the algorithm, we can classify cryptosystems into two categories – stream and block cipher. Some of the popular block ciphers are DES, AES, IDEA etc.

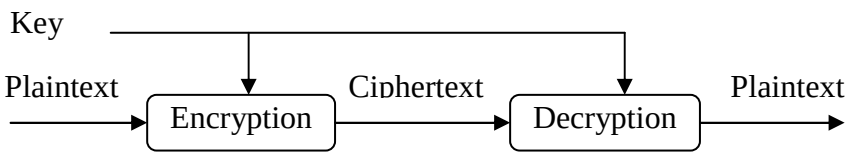

Figure 1: Block diagram for symmetric cryptosystem.

One of the most recent tools applied in cryptography is the theory of chaotic dynamical system [2-4]. Chaotic dynamical systems are very sensitive to initial condition and system parameter. Sensitive dependence is a valuable property for cryptography algorithm because if the initial conditions, used for encrypt data, are changed by a small amount; the cipher text should differ widely.

Public-key algorithms: Public-key algorithms are asymmetric, that is to say the key that is used to encrypt the message is entirely different from the key used to decrypt the message. The encryption key, also known as the public key, is used to encrypt a message but the person that has the decryption key, also known as the private key, can only decode the message.

Figure 2: Block diagram for asymmetric cryptosystem.

Digital signatures : The presence or absence of an authorized handwritten signature determines the authenticity of many legal, financial and other documents and photocopy do not count. For computerized message system to replace the physical transport of paper and ink documents, the only solution is digital signature. The problem of devising a replacement for handwritten signatures is a difficult one. Basically, what is needed is a system by which one party can send a signed message to another party in such a way that

- The receiver can verify the claimed identity of the sender.
- The sender cannot later repudiate the contents of the message.
- The receiver cannot possibly have concocted the message himself.

Secret-key signatures: One approach to digital signatures is to have a central authority that knows everything and whom everyone trusts, say Big Brother (BB). When sender A wants to send signed document (P) to receiver (B), receiver B generates $K_s(B, R_A, t, P)$ and send it where K_s ,R_A and t are secret key of sender A, random number and timestamp respectively.

Public-key signatures: A structural problem with using secret-key cryptography for digital signatures is that everyone has to agree to trust Big Brother. The most logical candidates for running the Big Brothers server are the government, the banks, or the lawyers. These organizations do not inspire total confidence in all citizens. Hence, it would be nice if signing documents did not require trusted authority. Fortunately, public-key cryptography can make an important contribution here. Let us assume that public-key cryptography encryption and decryption algorithms have the property that E(D(P))=P in addition to the usual property that D(E(P))=P. Assuming that this is the case, sender can send a signed message, P, to receiver by transmitting $E_r(D_s(P))$. Sender know own private key, D_s, as well as receiver public key, E_s, so constructing this message is something sender can do. When recipient receive the message, he transforms it using his own private key, as usual, yielding $D_s(P)$. He stores this text in a safe place and then decrypts it using E_s to get the original message.

5. CONCLUSION

Though present work deals with NEDR as a framework but certainly it helps in identifying the underlying issues with practicability especially at the level of rural entrepreneurs. Journey once commenced would certainly lead to a bright future to mankind. NEDR – being associated with common citizen would also help in increasing footfalls at CSCs/ Rural IT kiosk thus identifying these as public e-Gov front facet. The business model also encourages the sustainability aspect of the CSCs/ Rural IT kiosks.

REFERENCES

1. William Stallings, Network security essentials, Prentice Hall.
2. N K Pareek, Vinod Patidar and K K Sud, Discrete chaotic cryptography using external key, Physics Letters A, Vol. 309, pp. 75-82, 2003.
3. N K Pareek, Vinod Patidar and K K Sud, Block cipher using 1D and 2D chaotic maps, International Journal of Information and Communication Technology, Vol. 2(3), pp. 244-259, 2010.
4. CSI communication, May, 2002.

***Correspondence Author: Narendra K Pareek;** University Computer Centre, Vigyan Bhawan M L Sukhadia University, Udaipur (Raj) India.