Global Journal of Computer Science and Technology
Volume 12 Issue 3 Version 1.0 Fabruary 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Study on Efficient Digital Signature Scheme for E-Governance Security

By Mr. Nikhilesh Barik & Dr. Sunil Karforma
Burdwan University ,West Bengal ,India

Abstract - E-governance is the latest technological trend in the governance process all over the world whose application attribute can be Variety, Embedded, Rapidly, Year-round ,Simple, Moral, Ample, Responsive and Transparent i.e. in short VERY SMART processes are called E-governance. So for these system data should deliver speedy, space efficient, cost effective and secure way among other governments and its citizens.

This paper proposes a signed transmission scheme using standard RSA Digital Signature with implemented version of MD5 algorithm to ensure Message Integrity, Privacy, Nonrepudiation and Authenticity.

Keywords : *E-governance, RSA, Message integrity ,Digital Signature, Privacy, MD5.*

GJCST Classification: *D.4.6*

Strictly as per the compliance and regulations of:

A Study on Efficient Digital Signature Scheme for E-Governance Security

Nikhilesh Barik [α] & Dr. Sunil Karforma [σ]

Abstract - E-governance is the latest technological trend in the governance process all over the world whose application attribute can be Variety, Embedded, Rapidly, Year-round ,Simple, Moral, Ample, Responsive and Transparent i.e. in short VERY SMART processes are called E-governance. So for these system data should deliver speedy, space efficient, cost effective and secure way among other governments and its citizens.

This paper proposes a signed transmission scheme using standard RSA Digital Signature with implemented version of MD5 algorithm to ensure Message Integrity, Privacy, Non-repudiation and Authenticity.

Keywords : E-governance, RSA, Message integrity, Digital Signature, Privacy,MD5.

I. Introduction

Along with the development of Internet, the E-governance [8] has become a new pattern of activity for any Government. Almost all electronic transaction system used in E-governance needs a secure communication channel between the client and the server. During any type of these transaction ,we should involve a suitable cryptographic algorithm like RSA, DES, Elgamal, ECC etc. using Digital Signature (DS) where integrity, privacy, and non-repudiation can be imposed. Digital Signature works on the principle of public key cryptography[9]. Public key cryptography is based on a concept of key pairs, private key and public key. Public and private keys are nothing but large prime numbers generated by mathematical algorithms. The key pairs are used for both signing and encrypting the message. Public key helps to prove unequivocally that you are who you claim to be. The reliability of Digital Signature is same as that of a paper document with hand written Signature.

Now many of the government setting up the core infrastructure and policies to implement a number projects for their nation and state related to G2G concern like Income Tax filling, Banking Services, Provident Fund status ,passport & visa information ,Voter Id, National citizen card status, insurance & risk management ,pension plan status, details members of legislative, assembly and parliament ,trade license key or agreement, pan card verification, etc.

In E-governance[5] large amount of packets would be transferred between Government to Government using internet which is unsecure and time consuming. Intruders can change the information according to their requirements. So to ensure speedy communication and reduce the unauthorized access through information and communication technologies(ICT), it is required to use some techniques impose data Integrity, Privacy and Authenticity which must maintained with less communication costs using available bandwidth.

Section 2 describes Framework for signed G2G model. In section 3, proposed techniques has been discussed, Section 4 represents analyses of the proposed technique and implementation area. Section 5 draws a conclusion followed by references.

II. Frame Work of Signed G2G Model

G2G model implies simulations of Government to Government [5] services electronically. It can also be referred to electronic transaction between two or more governments, central to its states/provinces or one country to other,etc. It can be used to vertical and horizontal Governmental integration.

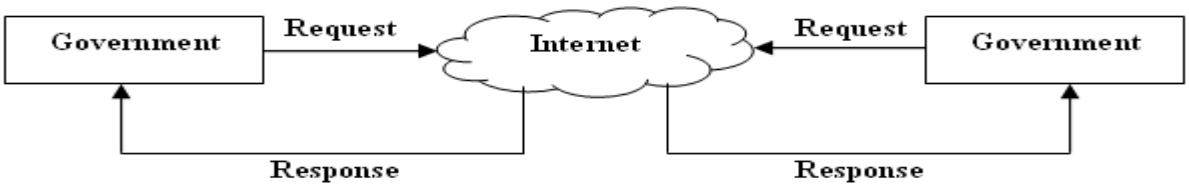

Figure 1: Simple model of G2G.

Author α : Research Scholar, Department of Computer Science , Burdwan University , West Bengal ,India
E-mail : nikhileshbarik@gmail.com_Mobile No: 09434516929
Author σ : Reader and Head , Department of Computer Science , Burdwan University , West Bengal ,India
E-mail : dr.sunilkarforma@gmail.com

So G2G is the online non-commercial interaction between two Government organizations, two departments of a Government organization.

Following block diagram shows the proposed scheme using Digital Signature to ensure Authenticity in any G2G model [1].

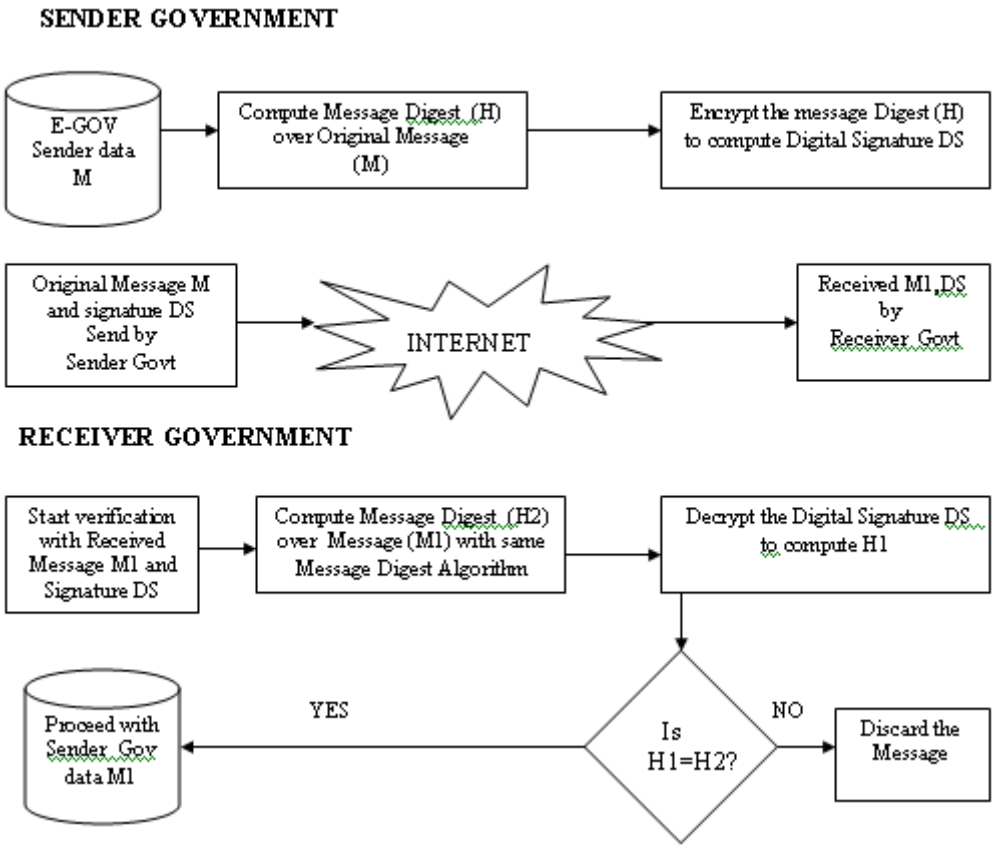

Figure 2 : Block Diagram of Digital Signature application to ensure Authenticity in any G2G model.

III. Proposed Scheme

Here Digital Signature [10] should be imposed by the sender government and Digital Signature should be verified by Receiver government in reality. First the message is hashed into a message digest. Using this hashed value a Signer (government) digitally signs (encrypt) the message (transaction) using his private key. This DS is attached to the original message and send by the sender Government.

After receiving the message, the receiver has to use the sender's public key to decrypt (we can say de-sign) the message digest and to ensures integrity authenticity. Confidentiality is achieved by comparing designed message and message digest using same algorithm used. As in an electronic transaction system an intruder should not be able to find out what transaction a particular user is executing if confidentiality is properly maintained. If the hash values of sender and receiver are equal, it serves to prove that the message has not been tampered. With changing even one letter in the message, the hash value would be changed. Hence message integrity is assured.

Non-repudiation is the cryptographic term describing the situation when the originator of a message cannot deny having sent it. Non-repudiation prevents from denying previous commitments or transactions from an entity.

a) Use Of Cryptographic Hash Implemented Version Of Md-5.

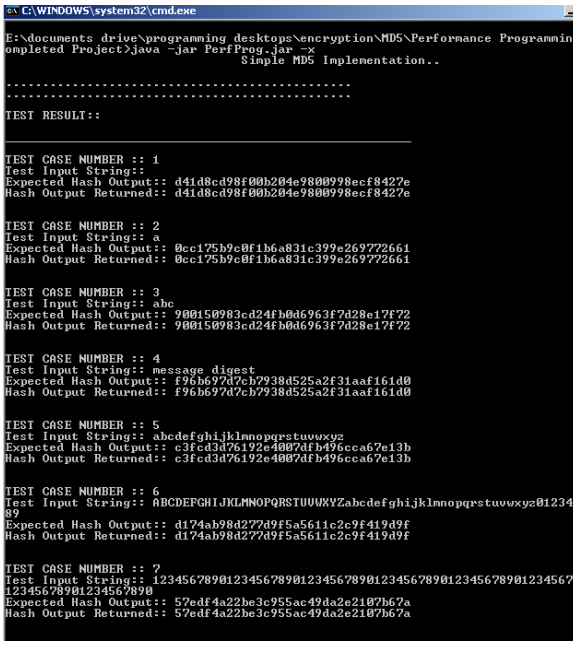

Figure 3 : Sample Output By Implemented Version Of Md-5 Hash.

Cryptographic hash function [6] will be used to verify the integrity of the data i.e. to ensure that the message has not been tampered with after it leaves the sender Government but before it reaches the receiver Government. So we perform the hash operations (some time called message digest algorithm) over a block of encrypted data to produce its hash, which is smaller in size than the original message[9,1].

Implemented Version of MD5 follows the all properties of standard hash function [2]. So when it operates on encrypted message M ,It returns a fixed-length hash value H. So that H = MD5(M).

No two messages produce the same message digest, otherwise message integrity violates. We are using Implemented Version of MD5 which performs better with respect to the standard MD-5 algorithm. Though standard output is generated and displayed in the above diagram but This Implemented Version of MD5 can be customize according to the requirements of the user. Here is the performance chart of Implemented Version of MD5 over standard MD5 for a certain hardware system.

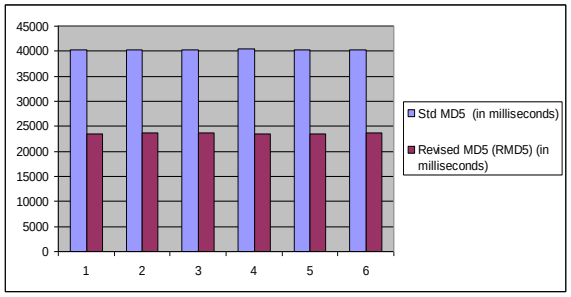

Figure 4 : Comparative study of time consumed (in ms) to create message digest by Implemented Version of MD5 and standard Java MD-5

i. All methods and classes are made final .
ii. Used System arraycopy for copying data into array.
iii. Pre-computed the String lengths and stored.
iv. Manually Implemented of the getHexString() Method.
v. Restructuring all the loops [4].

b) Digital Signature

Digital Signature [10] is one of the major development in network security . The need for Digital Signature has arisen with the rapid growth of digital communications. A Digital Signature algorithm authenticates the integrity of the signed data and identity of the signatory. Authentication in a Digital Signature is a process whereby the receiver of a digital message can be confident of the identity of the sender and/or the integrity of the message. RSA encryption is quite slow because of large key size and modular exponentiation operations that have to be used to ensure security. For the same reason, RSA's Digital Signature is slow as well [7]. The length of transmitted Signature equals the length of transmitted message. In other words longer the message, the longer the Digital Signature. So, the proposed scheme uses Secure Hash Algorithm[11] (MD5) to obtain condensed version of message, which will go as input for RSA Digital Signatures algorithm as shown in Figure-2. Properties like pre image resistant & collision resistant and the signing algorithm should sign on the message digest, rather than the original message are also maintained in this implemented version of MD5.

c) Hashed Rsa Digital Signature Generation Algorithm

Digital signing with RSA is roughly equivalent to encrypting with a private key. Basically, the Sender Government employee computes a message digest, then encrypts the value with his private key. The Receiver Government employee also computes the digest and decrypts the signed value, comparing the two. Of course, the verifier has to have the valid public key for the entity whose Signature is to be verified, which means that the public key needs to be validated by

some trusted third party or transmitted over a secure medium such as an authenticated courier.

Digital signing works because only the person with the correct private key will produce a "Signature" that decrypts to the correct result. An attacker cannot use the public key to come up with a correct encrypted value that would authenticate properly.

The RSA public-key cryptosystem can be used to authenticate another person. In general, the RSA algorithm is usually smaller than the private exponent . This means that verification of a Signature is faster than signing. This is desirable because a message will be signed by an individual only once, but the Signature may be verified many times. To make it faster modified Hashed-RSA Algorithm is presented as following. This algorithm takes Implemented Version of MD5 hashed data instead of plaintext.

The RSA scheme was the first implementation of public key cryptography. Let (α, n), (β, n) be the public and private key of a RSA cryptosystem. The Signature on the message is computes as follows:

Step 1. Sender Government uses Implemented Version of MD5 message digest algorithm to calculate H over message M, i.e $H = MD5(M)$.

Step 2. Now Sender Government once again encrypt the message digest H by the Private-key (α) of the sender Government to produce Digital Signature DS i.e. $DS = (H)^{\alpha} \bmod n$

Step 3. Now Sender Government send the original message M along with the Digital Signature DS to the receiver government.

d) Hashed Rsa Digital Signature Verification Algorithm

The verification process is just reverse of Signature generation process. At the receiver end we have signed message which contains RSA encrypted key and Digital Signatures.

Step 1. Receiver Government uses same message digest algorithm Implemented Version of MD5 to calculate another message digest H2 over received message M1, i.e $H2 = MD5 (M1)$.

Step 2. Now receiver Government uses sender government's the public key (β) to decrypt Digital Signature DS i.e. $H1 = (DS)^{\beta} \bmod n$

Step 3. Now receiver Government compare H1 and H2 .This failure of matching implies that document is not authentic or a possible computation error has occurred otherwise receiver government received correct and unaltered message from sender government.

IV. Analyzing the Proposed Technique

As there is general lack of awareness regarding the benefits of E-Governance as well as the process involved in implementing successful G2G (or G2G2G) projects, the administrative structure is not geared for maintaining, storing and retrieving governance information electronically and transactions are be made in non secured way. So day by day corruption is increasing from different ends. The privacy of each user and system data is of crucial importance for E-Governance system that meets user expectations and acceptance. Now a days each Government sector move away from paper documents with ink Signatures or authenticity stamps, Digital Signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory .

Some e-Governance projects can be implemented by this concept are :

i. **E-district** : Objective is to divide all states by e-district so that one actual district can have minimum one maximum any number of e-district with e-DM to run the every policy related to e-governance like e-Seva, which is already implemented in states like Andhra Pradesh and Rajasthan in India.
ii. **E-Tourism Card** : Any state /country can provide this card with duration so that any tourist can buy /issue this card for visit every tourist spot of that state/country.
iii. **E-Pay** : Every government should pay the monthly weight age (salary) by net banking though this have been implemented by many employer privately.
iv. **E-Coordination** : An application package is required to maintain all documents of very close interaction between the government department and the agency developing the solutions.
v. **E-Suggestion** : A team must require to understand and accept all suggestions from every end and forward those to proper places.
vi. **E-Health Card** : Government can provide this card to poor people for their health checkup in all district government hospitals.
vii. **E-Voting Card :** Any kind of decision where voting is required for different places of state or country can use this card.

Also the United States Government Printing Office publishes electronic versions of the budget, public and private laws, and congressional bills with Digital Signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with Digital Signatures.

V. Conclusion

The importance of high confidence is require for any kind of transmission of data in various department of any government sector and it is obvious in case of administrative decision and financial context. Also in

many scenarios the sender Government and receiver Government may have a need to show their higher authority that the message has not been altered during transmission. In this paper, we have proposed asymmetric encryption with Digital Signature to maintain data integrity customize hash function. The result will be more efficient when someone apply dual Digital Signature. VERY SMART concept is more applicable by ECDSA instead of RSA Digital Signature.

References Références Referencias

1. Barik Nikhilesh et al " Towards Design and Implementation of Space Efficient and Secured Transmission scheme on E-Governance data" ICCS- Nov 19-20,2010 Pages 80-85.
2. Kahate Atul "CRYPTOGRAPHY and NETWORK SECURITY, Second Edition,
3. Khan M.Ayoub and Y.P.Singh "On the security of Joint Signature and Hybrid Encryption" Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on,pp109-114
4. Matt Messier and John Viega" Secure Programming Cookbook for C and C++",O'Rilly Publisher.
5. Prabhu C.S.R " E-Governance concept and Case studies", PHI Learning Pvt Ltd,2009
6. Schneier Bruce, "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth), Publisher: John Wiley & Sons, Inc.
7. Stallings Williams, Cryptography and Network Security – Principal and Practices, Pearson Education.
8. http://en.wikipedia.org/wiki/Government_to_Government, 22nd october'2011
9. http://www.shadowtech-asp.net/examples/crypto ,22nd october'2011
10. http://en.wikipedia.org/wiki/Digital_Signature, accessed on 22nd october'2011
11. http://en.wikipedia.org/wiki/MD5 , accessed on 2nd october'2011

Acknowledgements

We would like to thank one of our BCA student Mr Rajarshi Dasgupta from "Durgapur Society of Management Science" to implement the MD5 algorithm and make comparative study with standard Java MD-5.