IJIRST –International Journal for Innovative Research in Science & Technology| Volume 4 | Issue 10 | March 2018
ISSN (online): 2349-6010

A Study on Importance of Digital Signature for E-Governance Schemes

Vishal R. Pancholi
Research Scholar
Pacific University,Udaipur, Rajasthan, India

Dr. Bhadresh P. Patel
I/C Principal
Matrushri L.J Gandhi (Bakorvala) BCA College Modasa, Gujarat, India

Dr. Dilendra Hiran
Principal
FCA, Pacific University,Udaipur, Rajasthan, India

Abstract

E-governance is the latest trend in many countries in which the government system is being online to deliver the government services to the citizens. The services can be from Government to Citizen (G2C) and Government to Business (G2B) or Government to Government (G2G) or Government to Employee (G2E) or vice a versa. People can access any application or any scheme from anywhere, anytime. As it comes with the word online, the biggest concern is the security issue. To provide E-authentication to the user there are many cryptographic techniques available. This paper discusses to increase the security, reliability, and non-repudiation of the user's data or information using Digital signature. It is highly secured and well-known method to authenticate and verify an electronic transaction.

Keywords: Digital Signature, Security, E-Governance, E-Authentication, MD5 Algorithm

I. Introduction

E-governance is the platform of Information and Communication Technology where all the government services have been delivered online, exchange information electronically, communication is done over the network and electronic transactions take place instead of the traditional system. There are so many entities involved in this E-governance system like a citizen, business, and government. There are many transaction models available involving all these entities. They are like Government to Citizen (G2C), Government to Business (G2B) or Government to Government (G2G) or vice a versa.

As much secure and confidential information is being passed over the network, it is required to provide security for the same. The Digital Signature is the method which is used to validate and authorize the content and users who are going to involve in the E-governance system. The Digital Signature assures sender's identity that is known as non-repudiation, the sender cannot deny that he/she has not sent the particular message of content or document.

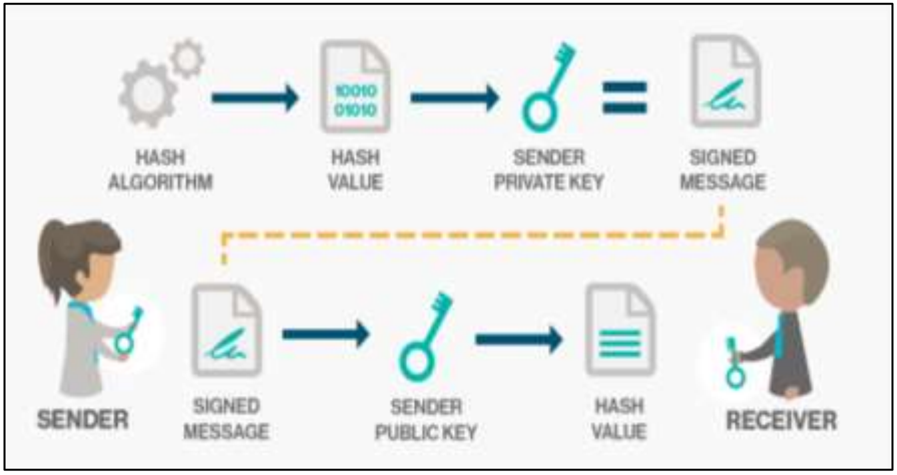

Fig. 1: Digital Signature Mechanism

Using any Hash algorithm, the hash value is generated and sender's private key is used to make it more secure. Now the signed message is passed by the sender and at the receiver side, the message is decrypted using sender's public key and again the hash value is applied to the message to read the original message.

II. LITERATURE REVIEW

In [1], they have concluded that cryptographic system cannot be considered as fully secured from the infringement attempts of the intruders, there will be the scope for further enhancements in the field of certificate generation and database management system.

In [2], Digital security is significant in E-Governance initiatives. Privacy of any transaction or information available on the network is essential. The important material or confidential data or information has to be protected from unauthorized users in E-Governance projects. Hence security is critical for successful implementation of such projects.

In [3], they have proposed asymmetric encryption using a digital signature to maintain data integrity using the customized hash function. They get a better result after implementing dual digital signature mechanism. They have applied very smart concept which is more applicable by ECDSA instead of RSA Digital Signature.

In [4], the proposed CL-EKM scheme to maintain data integrity and result in more efficient. The VERY SMART concept is more applicable to the proposed CL-EKM in an effective manner.

In [5], in this research paper the study of DSC, implementation of DSC, Message Digest algorithm, DSC work flow, and DSC risk is presented. The usage of DSC and implementation of Message Digest algorithm must be focused to make the e-Governance applications more successful in a developing country like India.

In [7], they had reviewed all researches on Digital Signature which is occurred in past one decade and recognizes the advantages and disadvantages of Digital Signature using Public key cryptography. They have revised all those techniques which will be developed or derived from the Digital Signature and are based on public key cryptography.

In [8], the proposed technique provides a way to shield the data, check the reliability and certification using best possible industry mechanisms. They introduce encryption, authentication of user by owner and other by cloud and verification of the digital signature of the owner.

In [9], they implement RSA algorithm with a digital signature in encryption to increase the security of users data or information. They want to work using safe communication on computers between systems to user.

III. IMPLEMENTATION

Here, n is the modulus, e is the encryption exponent and d is the secret exponent or decryption exponent. The algorithm is divided into 5 steps: Key Generation, Digital Signing, Encryption, Decryption and Signature Verification with their working functions are discussed as under:

A. *Step-1: Key Generation*

Randomly generate two large prime numbers: p and q.
Calculate $n=p * q$
Calculate the totient: $\Phi(n)= (p-1) * (q-1)$
Select an integer ‘e’ such that $1< e <\Phi(n)$ and $\gcd(e, \Phi(n)) = 1$
Calculate d, such that $d * e = 1 \mod \Phi(n)$
The public key is (n, e) and the private key is (n, d).

B. *Step2: Digital Signing*

Generate message digest of the document to be sent by using MD5 algorithm.
The digest is represented as an integer m.
Digital Signature S is generated using the private key (n, d), $S= m^d \mod n$.
Sender sends this signature S to the recipient.

C. *Step 3: Encryption*

Sender represents the plain text message as a positive integer m.
It converts the message into encrypted form using the receiver’s public key (e, n).
$C= m^e \mod n$
Sender sends this encrypted message to the recipient.

D. *Step 4: Decryption*

Recipient does the following operation:
Using his private key (n, d); it converts the cipher text to plain text ‘m’.
$m= C^d \mod n$

E. *Step 5: Signature Verification*

Receiver does the followings to verify the signature:
An integer V is generated using the sender’s public key (n, e) and signature S
$V= S^e \mod n$
It extracts the message digest M1, from the integer V using the same MD5 algorithm.

It then computes the message digest M2 from the signature S.
If both the message digests are identical i.e. M1= M2, then signature is valid.

IV. Experimental observations

A. *Step 1: Key Generation:*

1) We have chosen two distinct prime numbers p=23 and q=53.
2) Compute n=p*q, thus n=23*53 =1219.
3) Compute Euler's totient function, Ø(n)=(p-1)*(q-1), thus Ø(n)=(23-1)*(53-1) = 22*52 = 1144.
4) Choose any integer e, such that 1 < e < 1144 that is gcd (e, 1144) =1. Here, we chose e=3.
5) Compute d, d = e-1(mod Ø(n)), thus d=3-1(mod 1144) = 763.
6) Thus the Public-Key is (e, n) = (3, 1219) and the Private- Key is (d, n) = (763, 1219). This Private-Key is kept secret and it is known only to the user.

B. *Step 2: Encryption:*

1) The Public-Key (3, 1219) is given by the Cloud service provider to the user who wishes to store the data.
2) Let the message to be send is "hello" which is converted to integer in the following manner:
   A=0, B=1 ,a = 27, b=28,c=29 and so on.
   So the message "welcome" is encoded to m= 49313829413931
3) Data is encrypted now by the Sender using the corresponding Public-Key which is shared by both the sender and the receiver.
   C=m^{e}mod n=C=49313829413931^{3}(mod1219) = 625535179657807535.
4) This encrypted data i.e., cipher text is send to the recipient.

C. *Step 3: Digital Signature and Signature Verification:*

1) First using MD5 algorithm the message gets converted to message digest i.e. to hexadecimal form.
2) MD1=H(m)= 0x000c00f0000000f0426f00f0726000f0.
3) Message digest in decimal form M1= 01202400002406611102401141080240.
4) Next digitally signed the message digest MD1 using its own private key d to generate digital signature S.
5) S=(MD1)dmod n= 0887025800025883929602588501240258.
6) Sender then sends the digital signature S to the recipient.
7) Receiver then computes the integer V using S, e and n.
8) V= S^{e} mod n= 01202400002406611102401141080240.
9) Receiver the computes the message digest from S using MD5 algorithm
10) MD2 = 01202400002406611102401141080240.
11) Since V = MD2, so the Signature is verified.

D. *Step 4: Decryption:*

1) The receiver decrypts the data by computing, m = C^{d}(mod n) = 49313829413931.
2) Once the m value is obtained, user will get back the original message using the same encoding technique.

Some of the E-governance schemes that can provide security by implementing this type of algorithm to their users:

- E-payment: Every government should use this feature to get/receive the payment for the services offered by them.
- E-Tourist card: Tourists can get tourism card to visit any state/country from one portal only.
- E-Training: Any academic or professional training can be provided and more and more employees can get benefits from single place.
- E-Learning: The wide range of learning materials, audio, video will be provided through this medium and learners and tutors across the world can join this forum.

V. Conclusion

As the E-governance system is very wide and connected with citizens, business or another government, it must require maintaining the security concerns in any electronic transaction. There are so many cryptographic techniques available to provide the security. In this paper, it is shown the use of digital signature in many government projects. It is also described how digital signature is implemented using the MD5 algorithm.

References

[1] Abhishek Roy1, Sunil Karforma "Authentication of User in E-Governance: A Digital Certificate Based Approach" International Journal of scientific research and management (IJSRM) Volume-2 Issue-8, Pages 1212-1221, 2014, ISSN (e): 2321-3418

[2] Shailendra Singh Member, IEEE; D. Singh Karaulia "E-Governance: Information Security Issues" International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya Dec-2011

[3] Nikhilesh Barik & Dr. Sunil Karforma "A Study on Efficient Digital Signature Scheme for E-Governance Security" Global Journal of Computer Science and Technology, Volume 10 Issue 3, February-2012 Online ISSN : 0975-4172

[4] F.Jerlinmary, Dr.M.Deepamalar "Advanced E- Governance Security Using Certificate less Effective Key Management" International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 6, June 2017, ISSN(Online): 2319-8753

[5] Shaikh Imtiyaj, Er. Ratan kumar Agrawal, Dr A K Hota "Digital Signature Certificate: A Great scientific Knowledge for Nation Development" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. IV. (Jul.-Aug. 2017), PP 56-60

[6] Yong Huang, Fugui Chen, Peixin Qu "Research on Digital Signature Based on Digital Certificate" School of Information Engineering, Henan Institute of Science and Technology, Xinxiang, 453003, China

[7] Shivendra Singh, Md. Sarfaraz Iqbal, Arunima Jaiswal "Survey on Techniques Developed using Digital Signature: Public key Cryptography" International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 16, May 2015

[8] Nagendra Kumar, Ashok Verma, Ajay Lala "Access, Identity and Secure Data Storage in Private Cloud using Digital Signature" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2014 ISSN(Online): 2320-9801

[9] T. Sivasakthi, Dr. N Prabakaran "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2014 ISSN(Online): 2320-9801

[10] Wojciech Kinastowski "Digital Signature as a Cloud-based Service" CLOUD COMPUTING 2013: The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization

[11] Dhruvi Chaudhary, prof.Rakesh Shah "A Survey on Digital Signature with RSA encryption algorithm to enhance the Data security of cloud in cloud computing" International Journal for Innovative Research in Science & Technology, Vol-3Issue-8, 2016

[12] Mr. D.Shiva, Rama Krishna "Providing Security to Confidential Information Using Digital signature" International Journal for Innovative Research in Science & Technology, Vol-2 Issue-6, 2015